地域医療連携情報システム構築
ハンドブック 2010

―IHE XDS による HIE（Health Information Exchange）の構築―

2010 年 3 月

ePHDS 委員会/日本 PACS 研究会

日本 IHE 協会　編

目次

執筆者一覧

・第 1 章
安藤　裕　　放射線医学総合研究所　重粒子医科学センター医療情報室

・第 2 章
細羽　実　　京都医療科学大学

・第 3 章（3.1～3.5）
大林　正晴　　株式会社　管理工学研究所

・第 3 章（3.6）
山本　裕　　横河医療ソリューションズ株式会社

・第 4 章、附属書 G
谷川　琢海　　放射線医学総合研究所　重粒子医科学センター医療情報室

・第 5 章、附属書 F
野津　勤　　理工学振興会

・第 6 章
喜多　紘一　　東京工業大学

・附属書 A、附属書 C、附属書 D
向井まさみ　　放射線医学総合研究所　重粒子医科学センター医療情報室

・附属書 B、附属書 E
高橋　正人　　株式会社　管理工学研究所

・編集
森口　修逸　　株式会社エム・ピー・オー

1. はじめに

このハンドブックは、地域連携システムや施設間連携システムを構築する方法について、医療関係者の方を対象に解説してあります。特に、これから連携システムを構築する必要がある人にとって、発注などに際して、役に立つ内容になっています。また、システムを購入するときにシステムメーカに提出する必要がある仕様書が、楽に完成できるような内容となっています。

このハンドブックは、地域医療連携情報システムの取り扱うデータの中身については、詳しく触れません。なぜならば、目的とする連携システムが脳卒中の患者さんを対象としたり、周産期の患者さんを対象としたりするなどの違いにより、データの中身は大きく変化する可能性があるからです。連携をするための情報システムの枠組みを提示しているわけです。この枠組みをベースにして、読者の方々は各々の目的に合ったデータを定義して下さい。また、詳細な運用の流れなども検討する必要があります。

私たちが地域医療連携情報システムを検討したときに、一番問題になったのは、連携をする組織をどのように構築するかです。どんなに良いシステムがあったとしても、人と人との信頼関係の築かれた組織がなければ、地域医療連携情報システムが活用されることはあり得ないでしょう。いかに気心の知れた人のつながりのある組織を構築するかにかかっていると言っても過言はないでしょう。地域医療連携情報システムを検討している方は、この点についても十分に組織の検討を行う必要があります。

1.1 このガイドブックの読み方

第２章の地域医療連携情報システムの目的と構築の方法には、まず、2.1　連携システムの概要が書いてあります。この部分を読めば、想定されている連携システムの目的や地域連携パス、病診連携、遠隔画像診断などの応用システムの概要が理解できます。

第３章は、システム構築の要求仕様について記載してあります。システムをあるメーカから購入する場合に、メーカに渡す仕様書の内容について、解説してあります。この仕様は、IHE（Integrating the Healthcare Enterprise：１．２ IHE の概念を参照）の考え方に従っています。また、この章には、本来の情報の共有機能だけでなく、データの保護やアクセスコントロールなどのセキュリティ面のことも書いてあります。

ぜひ、これらの仕様を利用して、要求仕様書を完成させて下さい。

第４章は、厚生労働省から出ている安全管理ガイドラインの内容に触れています。よりセキュリティを高めたいときには、必読の章です。

第５章は、連携をする組織を作って、その管理・運営をどのように行うかが

記載されています。システムを作ってもそのシステムに魂が入っていなければ、うまく動作しないことは火を見るより明らかです。運営をスムーズに行うために最低限しなければならない事務局機能が述べられております。

第６章は、今後の新しいコンセプトしての「電子私書箱」構想が解説されています。医療分野で電子私書箱を利用して、地域医療連携情報システムを構築することのメリット・デメリットなどを検討しています。

後の附属書 A には、施設間情報連携統合プロファイル XDS のユースケース、附属書 B には XDS の概説、附属書 C にはセキュリティ関連の統合プロファイル ATNA,CT の解説、附属書 D には、ATNA のログの例、附属書 E には、関連する統合プロファイルのオープンソースの利用方法、附属書 F にはコミュニティの構築の手順、ポリシー、附属書 G にはベンダからの提案依頼項目について記述しています。

これらのことを上手に利用して、地域連携システムや施設間連携システムを構築できることを願っています。

1.2 IHE の概念

IHE の目指すことは、医療分野における IT 化・標準化の推進を通じて医療安全や医療の質の向上です。その活動は、一般には IHE サイクルと呼ばれており、「医療機関における様々な部門における複雑な問題」を解決します。医療機関におけるいろいろなシステムに関する問題点を解決するために、メーカの技術者と協力して業務の流れを分析して、他の医療機関でも適応可能な『業務の手順書』を作成します。

この手順書を既存の標準的な規格を元に、システム間の情報の流れを定義し、IHE のテクニカルフレームワークと呼ばれる規格書を作成します。作成されたテクニカルフレームワークに則り、各メーカは製品に組み込み接続テストを行います。接続テストの結果は、「一覧表」として IHE 協会のホームページ上で公開されています。この表から自分の施設に必要な装置やシステムを探して、『業務の手順書』を参考に仕様書に引用すれば、システムを円滑にかつ迅速に導入することが可能となります。

この IHE が作成している『業務の手順書』のうち、このハンドブックが対象としている地域医療連携情報システムに応用可能なものがたくさんあります。その中心が、情報共有のための『業務の手順書』である、XDS (Cross-Enterprise Document Sharing) と呼ばれるものです。この機能は、中央の一カ所に索引機能のサーバをおいて、医療情報を共有するときには、誰々さんのいついつの退院サマリをどこのサーバに保存したかを中央の索引サーバに登録します。

一方、情報を参照するときには、中央の索引サーバを利用して、この患者さんのいついつの退院サマリは、どこにあるのかを検索し、その所在がわかったら、直接、保存してある保管サーバから情報を引き出します。

XDS は、このような索引サーバと保管サーバが組となった枠組みを使用してい

ます。

1.3　アメリカやヨーロッパの地域連携システム

日本では、地域連携システムは、未発達ですが、世界に目を移すとアメリカやヨーロッパでは、すでに地域連携システムが立ち上がって稼働しています。図 1-1 に示すように、１８以上の国や地域で地域連携システムが IHE の XDS の枠組みを利用しています。アメリカでは、フィラデルフィアプロジェクト、カナダではインフォウエィ、英国の放射線診断連携、フランスの DMP、スイスのサンクトガレンなどです。

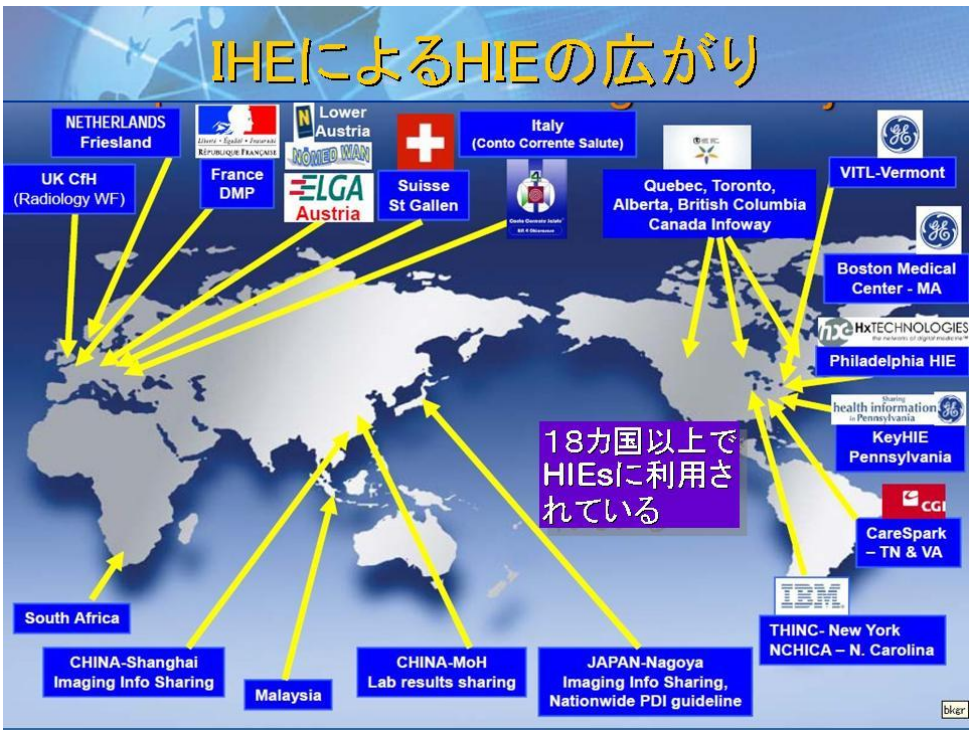


図 1-1　IHE XDS による地域連携システムの広がり

1.4　なぜ IHE？

IHE の概念は、『医療分野における IT 化・標準化の推進です』と書きました。なぜ、IHE なのでしょうか？地域連携システムや施設間連携システムを構築する方法には、IHE 以外に方法がないのでしょうか？

たしかに、IHE 以外の方法で地域連携システムや施設間連携システムを構築する方法は、たくさんあります。それでは、なぜ IHE XDS の枠組みを利用して地域連携システムを構築するとどんな便利な点があるのでしょうか？その答えは、標準化です。IHE は、利用形態を多くの医療機関で利用可能な業務の流れとしてまとめ『業務の手順書』を作っています。これが、第１レベルの標準化です。次に、この『業務の手順書』をもとに、既存の標準規格を用いて、情報の内容

や情報の伝達方法などを決めます。これが第２レベルの標準化です。ここでできた定義書を元に、１年に一度接続テストを行い、メーカが作ったシステムが実際に他のシステムとデータのやり取りができるかを調べます。これが第３レベルの標準化です。

他の方法で、これら第１レベルから第３レベルまでの標準化を行っている規格団体は、ありません。そのため、他の方法で地域連携システムを構築してしますと、将来、他の地域連携システムと接続しようとした場合に、大変な労力と長時間の接続調整が必要となる可能性があります。IHE の XDS の枠組みを利用することにより、これらのリスクを回避することができるのです。

標準化が地域連携システムには、絶対に必要です。メーカの独自の方法でシステム連携を行うと、将来、他のシステムと接続する場合に、膨大な費用と時間がかかる可能性があることを、記憶に留めておいて下さい。

1.5　今後の進展

2009 年度に厚生労働省が開始した地域医療再生基金によって、今後は、地域連携システムの普及が期待されます。日本のいろいろの都道府県で、様々な地域連携システムのニーズはあります。IHE の XDS を上手に利用して、このニーズを解決することができます。各都道府県に地域連携システムができた後、今度は、都道府県をまたがったシステムが必要になるときが来るでしょう。その時に、各システムを接続する問題が生じる可能性があります。

繰り返しになりますが、地域連携システムを構築するときには、標準化が必要であり、将来の拡張性を考慮して標準的なシステム構築を行うことが解決策です。現在、地域連携システムを計画している方々は、くれぐれも標準化を心がけて下さい。

1.6　今後の改訂

本ハンドブックは、今後、技術の進歩により内容が古くなる可能性があります。また、セキュリティポリシーや各種のガイドラインが改訂されることにより、内容がこれらのポリシーなどと異なることが予想されます。

ePHDS 委員会/日本 PACS 研究会および日本 IHE 協会では、今後随時内容を改定する予定ですので、日本 PACS 研究会や日本 IHE 協会のホームページ等で改訂版の有無の確認をお願いします。

是非、最新版のハンドブックをご利用下さい。

2. 地域医療連携情報システムの目的と構築の方法

本章では、地域医療連携情報システム(以下、連携システム)の目的と概要について述べ、システムの基盤を構築する方法として、IHE によるシステム構築がもつ利点を解説する。

2.1 連携システム

本節では、連携システムの目的と概要、基盤システムの分類について紹介する。

2.1.1 連携システムの概要

2008 年 4 月から始まった新たな医療計画では、4 疾病（がん、脳卒中、急性心筋梗塞、糖尿病）5 事業（救急、災害、僻地、周産期、小児）ごとに医療連携ネットワークを構築することが求められている。脳卒中、癌、循環器疾患、糖尿病など疾病別に発生から診断、治療、リハビリまでを診療ガイドラインに沿って作成する一連の地域診療計画は地域連携クリティカルパスと呼ばれる[1,2]。これらの連携が効率的に実施されるためには、各医療機関が IT 化され、各施設間で医療情報がスムーズにやり取りできる環境が確立されなければならない。即ち、各医療機関の電子カルテに他の医療機関の情報が、必要に応じて取り込まれたり、読み出されたりする基盤（インフラストラクチュア）の構築が求められる。現状では、2 割程度の IT 化率であり、まだ発展途上である。

医療情報を共有する IT 基盤には、可搬型媒体による方法、ネットワークによる方法がある。ネットワーク型では 1 対 1 の通信による情報伝送（Information Exchange）と、情報を共有できるネットワークを構築する方法（Information Sharing）に分けて考えることができる(表 2-1)。

表 2-1 医療連携システムの種類と IHE 統合プロファイル(後述)

医療連携システム		IHE 統合プロファイル
情報交換型 (Information Exchange)	可搬型	PDI、XDM
	1 対 1 ネットワーク型	XDR
情報共有型 (Information Sharing)	ネットワーク型	XDS

2.1.2 可搬型媒体による連携

可搬型媒体による連携は、情報交換型（Information Exchange）になる。可搬型媒体で情報を交換する場合には、相手を特定することなく患者が自らの意思と責任で情報を運ぶ。標準的なフォーマットが定まれば（後述の IHE　PDI など)、連携運用が始めやすいという利点がある。しかしながら、読み出す際の障害など、トラブルの発見に時間的な遅れが生じ、問題解決に時間がかかってしまうという欠点がある。もしある施設で発行した全てのメディア共通の問題で

あったとすると、大量に問題メディアが出回る結果を招く。また持ち込まれた施設は、データを保管することにより大量の連携データを保管することになる場合も考えられる。また、多くの種類の可搬型媒体への対応も必要である。そのため、安定した可搬型媒体による連携の運用のためには、後述のネットワークによる場合と同様の運用の取り決めが必要である。そのために基本的な申し合わせ事項も決められている。

地域連携クリティカルパスにおいて、複数の医療機関、複数の医療スタッフが 1 人の患者に同時に対応することが必要な場合、あるいは救急時に対応するには、可搬型媒体だけによる連携には限界があると考えられる。

2.1.3 ネットワークによる連携

遠隔画像診断支援のための連携では、情報交換型（Information Exchange）として 1 対 1 の伝送が行われるケースが多い。これは予め決められた医療機関間で通信が行われるものであり、互いに合意した安全な伝送手段を用いて行われる。ネットワーク型の医療連携は、その瞬間に相手を確認して通信に移るため、直接的であり曖昧さがない状態で行なわざるをえない。従って、問題があれば即座に見つかり、解決への動きは早い。ネットワークセキュリティ、責任分界点(ガイドラインの遵守）の取り決めなどへの対応が必要であることは言うまでもない。

一方、中央にサーバを置いて、各医療機関のもつ連携患者の医療情報を一括管理し、各医療機関が情報を共有、追加登録するという形は、情報共有型（Information Sharing）に分類される。この方式では、連携地域内で長期に渡って情報共有することが可能となる。現在、多くの電子化された医療連携ではこの方式が使われている。これに加えて、医療機関にある情報の所在情報を一括管理し、個々の情報は参加する医療機関内に存在する形でアクセスすることも可能である。この場合、所在情報だけの管理を 1 箇所中央で持てばよいことになる。ただし患者 ID のマッピング基盤は必要である。またセキュリティ基盤の確立、責任分界点の対応、共通の考え方（ポリシー）に同意するコミュニティの形成と運用組織が必要であり、設置のハードルは高くなる。しかしながら、この基盤は長期に渡って効果的な共有を可能とすることができ、本稿では、この基盤を IHE の手法を用いて確立する方法を中心に解説を進めていくこととする。表 2-2 にそれぞれの方式の特徴を比較した。

表 2-2 医療連携システムの形式比較

医療連携システム		通信相手	トラブル発生	設置ルール
情報交換型 (Information Exchange)	可搬型	不特定	後日	申し合わせ
	1対1 ネットワーク型	特定	即時	互いの合意
情報共有型 (Information Sharing)	ネットワーク型	特定の メンバ間	即時	コミュニティで合意

2.2 IHEによる連携システム構築

本節では、IHEによる手法を用いた連携システムについて概説する。

2.2.1 医療連携のシナリオ

一般に、コミュニティが成立するには、メンバが共通の考えに同意し、共通の言葉が話せ、共通の手続きに同意していることが前提となる。一方、自然発生的に形成されるコミュニティは、その中で意志を持って標準的な手続きを定めることはない。ところが、コミュニティが次々と発生し、コミュニティ間での物や情報の交換に利便性が見出されると、共通の物を特定する共通の言葉の必要性が認識され始める。複数のコミュニティ間で交流が進むと、手続きは膨大かつ複雑となり、どの相手とも共通の手続きと情報交換の言葉が必要となってくる。即ち、情報の交換の価値を認識するところから標準化が始まると考えられる。従って、医療連携を行うコミュニティでは、どんな時にどんな情報を交換し、共有したいかを明確にし、合意するところから始める必要がある。

例えば、医療機関A、B、C、Dがあり、患者はA機関で救急の治療を受け、B機関に入院、C機関で長期療養を行い、近隣の診療所Dで診療を受ける場合を想定する。診療所Dの医師は、患者から過去の治療経緯を聞くだけではなく、医療機関A、B、Cから必要な医療情報を参照したいと考える。このシナリオを実現するためには、医療情報を一箇所に集中させて管理し（管理センタの設置）利用する方法がある。医療機関は患者の同意を得て管理センタに情報を送信する。関連医療機関は必要に応じて、医療情報にアクセスすることになる。しかしこのような大規模な管理センタの設置は多大の初期コストを伴う。そこで、例えばコミュニティの内部に情報の所在管理だけを行うセンタを設置し、実際の情報は各医療機関が保管しておく。診療所Dに行った患者の過去の情報がどこにあるかは、所在管理センタへの問い合わせで即座に知ることができる。図2-1にそのシナリオ例を掲げた。患者が医療機関を転々とする状況は同じであるが、コミュニティの中では、患者はどの医療機関に行っても、医療機関は所在情報にアクセスして情報の在り処を知り、過去の医療情報を利用することが可能となる。

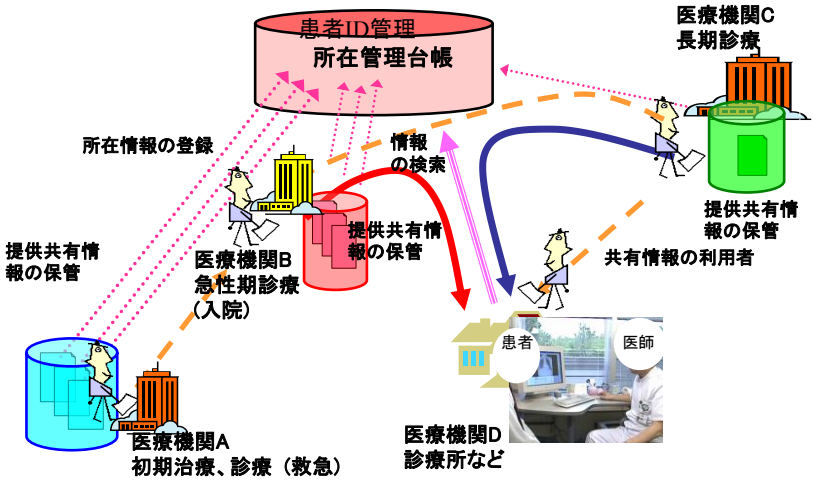


図 2-1　医療情報連携のシナリオ例

2.2.2　処理機能の単位と情報交換手続き

このように医療連携のシナリオが定められると、その中で重要な役割を果たしている処理機能をひとつのユニット(単位)として抽出し（これをアクタと呼ぶ、処理装置とみてもよい）、シナリオをより一般化する。図2-1を構成するシナリオの処理機能部分（アクタ）は、所在管理台帳、提供共有情報の保管、情報の利用機能、である。情報を提供する仕組みを考えると、図2-1に加えて情報を供給する元となる機能が必要になるし、患者のIDは医療機関ごとにばらばらなため、患者IDの照合と特定が必要となり、患者ID管理機能が必要になる。以上の処理機能を抽出すると図2-2のようになる。これらは処理機能のユニット(一単位)であり、アクタと呼ばれるものである。

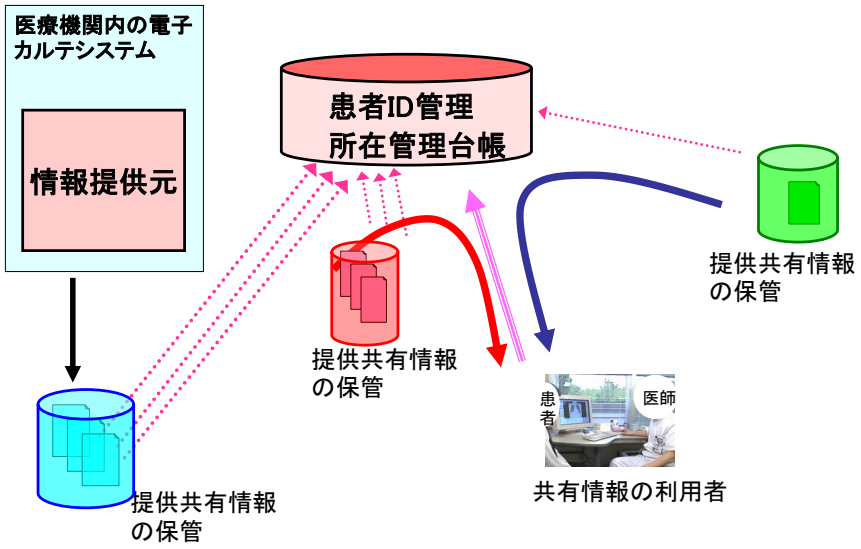


図 2-2　医療情報連携の処理機能の抽出

処理機能(アクタ)が抽出できると、次にこのシナリオを実際に目論見どおりに動かすためには、アクタの間でどのような情報のやりとりが必要かを決めなくてはならない。標準的に情報の交換を行うには、通信規約と用語コードを定める必要がある。アクタを実装しようとする複数のベンダが参加できることがこのシナリオの普及構築に必要な要件であり、競争が成り立つ環境が期待できる。そのためには、情報交換の手続きの標準化が必須である。

2.2.3　IHE が優れている点

処理機能(アクタ)の間の情報交換手続きは、シナリオの目論見を達成するために意味のある情報のやり取りを決めることでなければならない。単にあるアクタとあるアクタの間だけの1対1の情報交換だけを取り決めるだけではなく、所在管理台帳、共有情報の保管、情報の利用などの各アクタが連携して統合的に情報が取り扱えるような決め方が必要となる。つまり、情報共有シナリオを実現するために最もバランスのとれた整合性のある情報交換手続きを取り決める必要がある。これがIHEという新たな標準化の考え方であり、機能単位間の接続だけを規格で定めることに留まっていた従来の標準化との決定的な違いである。

医療情報の標準規格の中でもDICOMと呼ばれる規格は、最も成功した事例とされており、世界的に普及をしているが、一方では実装に当たっての問題も出てきた。標準規格は、あらゆる場面で使われることを想定しなくてはならないというのが宿命である。そうなると膨大な場合分けとその取り決めを行っていかなければならない。しかも、その膨大な選択肢ゆえ、規格の実装段階ではその選択に大変な手間がかかる。最終決定をするのはユーザ側であるが、その選択肢の意味を説明する側の労力も大きく、また双方が合意を形成する時間は計

り知れないものとなる。多くのトラブルの原因は、意味を説明する側の失敗、あるいは聞いている側の誤解によるものであった。根本的には、判断する側が最終的にどんな業務を効率化したいかという明確な目的がなかったためであり、また目的があったとしても、それと標準の選択肢とがうまく結びつかないためであった。

システム構築には、何がやりたいかのシナリオづくりと、それを成り立たせる機能単位(アクタ)の特定と、それらが共同でなしえる情報処理のための情報交換の統合的な設計が必要とされる。DICOM、HL7という医療情報の標準規格が整備されてきたにも関わらず、標準化が進まないのは、その点が十分取り上げられなかったためである。そこで、①共通のシナリオづくり、②処理機能(アクタ)の特定、③ユニット間の情報交換の標準化というステップを明確に仕様化する動きが出てきた。これがIHEである[3,4,5,6]。

2.2.4 IHE の手法

IHEにおける共通のシナリオ作りは、各医療機関の独自の情報化ではなく、共通した業務処理に基づくものであり、そのシナリオがより広く使われる可能性を追求するものである。アクタの特定は、実装する際に最低限共通業務をこなすのに必要な機能の単位であり、どの装置にどう実装するかの選択を容易にする。また標準的な情報交換は、異なるベンダの実装した機能単位と共通に接続できるものであり、ユーザが本来何の考慮もいらない部分である。

IHEでは、共通のシナリオを記述する際、そのアウトラインを書いたものをプロファイルと呼んでいる。共通に使えるもの、各医療機関で、あるいは医療機関連携で使えるものであり、かついくつかの要素を組み合わせ統合したものという意味で、これをIHEでは、Integration Profile(統合プロファイルと訳す、以下プロファイル)と定義する。

次に、登場した処理機能ユニットをアクタ（Actor）とする。舞台で演技する、あるいはシナリオを展開する役者に準えている。アクタが共通にしゃべる言葉、しゃべる様式、即ち情報交換手続きをTransaction（以下トランザクション）と呼んでいる。共通シナリオを記述する統合プロファイルは、アクタとトランザクションで構成される。これがIHEのモデル化の手法である。ユーザ側は、プロファイルが何の共通シナリオを実現するものかを知り、ベンダに注文することになる。その際には、仕様（後述のテクニカルフレームワークに記述される）は唯一であり、ベンダーユーザ間で誤解を起こす点はない。

表 2-3 IHE によるモデル化の言葉のアナロジー

舞台	場面	登場人物	会話
現場の業務	共通シナリオ	処理機能ユニット(装置)	情報のやりとり
IHE	統合プロファイル	アクタ	トランザクション

2.2.5　医療連携の IHE

既に紹介した医療連携シナリオをIHEで説明してみる。このシナリオ全体を施設間医療連携プロファイルと名づける。英語では、Cross Enterprise Document Sharing Integration Profileと呼ばれている。Enterpriseというと企業体をイメージするが、医療機関のことである。Documentは公式な文書であり、コンピュータファイルでもあるが、ここでは医療情報を表わしている。プロファイルの略号(コード名)をXDSという。医療連携は医療情報共有、医療情報交換などととらえ、HIE (Health Information Exchange)と表現されている。IHEからもじったと思われがちであるが、実はHIEの方がIHEより先に定義されている。以下、簡単にIHEによる医療連携を「IHEによるHIE」と呼ぶことにする。

XDSプロファイルでは、アクタ、トランザクションは図2-3のように構成される。所在管理台帳は、Document Registry(ドキュメント・レジストリ)となり、提供共有情報の保管はDocument Repositry(ドキュメント・リポジトリ)、情報提供元はDocument Source(ドキュメント・ソース)、共有情報の利用者はDocument Consumer (ドキュメント・コンシューマ) というように名前がつけられている(表2-4)。このようにIHEでは共有シナリオをアクタとトランザクションでモデル化し、文書化を行っている。

表 2-4　情報共有プロファイルにおけるアクタ名の対応

処理機能ユニット	所在管理台帳	提供共有情報の保管	情報提供元	共有情報の利用者
アクタ名	ドキュメント・レジストリ	ドキュメント・リポジトリ	ドキュメント・ソース	ドキュメント・コンシューマ
英語名	Document Registry	Document Repository	Document Source	Document Consumer

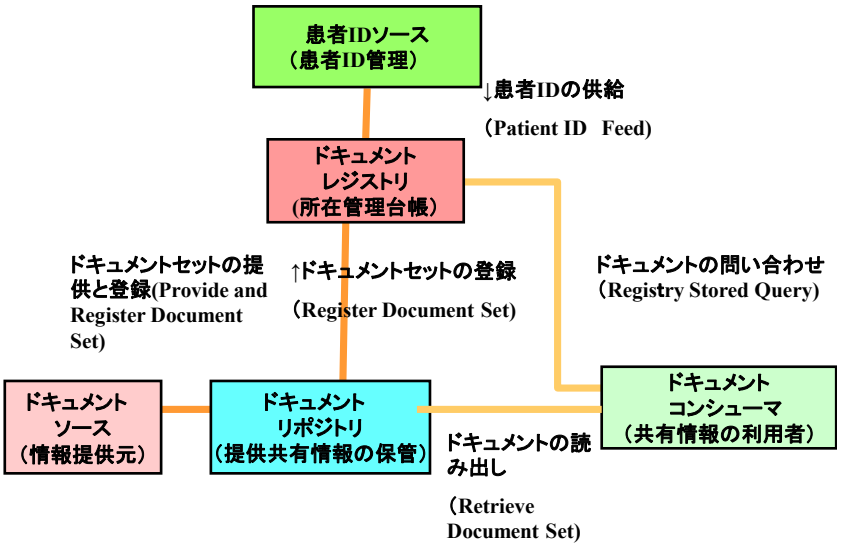


図 2-3 XDS 統合プロファイル

2.2.6 従来型の医療連携と IHE の比較

地域医療連携システム構築に当たって、IHEによる方式と従来のWebサーバによる方式と比較してみると表2-5のようになる。

表 2-5 医療連携システム構築における IHE の特徴

仕様	特徴
集中サーバ型	・医療情報を全て集中管理 （データのメンテナンスはセンタで行う） ・Web サーバに対してネットワーク経由でアクセス。インターネットバンキングなど様々なインターネット経由のサービス形態と同じ ・どの利用者も同じ Web アプリで閲覧する。 ・データを登録する時に標準化されていると便利。利用するときは、標準化は不要。 ・データを取り込んで利用することは困難 ・簡単に構築(ホームページを開くのと同じ)
所在管理サーバ＋分散管理サーバ型（IHE）	・所在情報をセンタで管理(レジストリ：センタは所在情報の管理）、実際の情報は分散管理(リポジトリ）（参加する医療機関が自らのデータを管理） ・Web サービスの仕組みを利用（SOA: Service Oriented Architecture） ・利用する側がアプリを自由に作る ・データを登録する際もデータを利用する際も標準化が必須 ・データを取り込んで利用することができる ・標準への準拠、一貫した用語コードのメンテナンスが必要 ・セキュリティを確保する手法も標準化されるので、ガイドラインへの適応が評価しやすい。

このように、IHEによるHIEの特徴は、分散型をとることが可能であり（無論集中型にすることも可能であるが)、センタの負荷が小さく、多くの医療機関の連携に適している。また、共有する医療情報を単に閲覧するだけでなく、自施設に取り込み利用することが可能となるという大きな特徴をもつ。そのための標準化が自施設のシステムに求められることは言うまでもない。さらに、安全管理ガイドラインに記載されたセキュリティ対策ができているかどうかに対して、一定の評価を与えることが容易になる。

2.2.7 テクニカルフレームワーク

共有シナリオを記述し、アクタを定義、トランザクションの詳細は標準規格を用いて記述された仕様書をテクニカルフレームワークと呼んでいる。共通シナリオ、即ちプロファイルを構成するアクタは共有場面ごとにある程度役割のバリエーションがあるが、トランザクションは決められた情報を相手に伝えるため厳密に定義され、標準規格を用いて記述されている。この記述はベンダが実装可能な仕様書でもあり、IHEによる実装のための仕様書である。

IHEは、このテクニカルフレームワークを策定し、インターネットを通じて世界に公開することで、標準化を進めている。即ち、IHE テクニカルフレームワークは技術仕様書であり、標準規格の適用ガイドとなっている[3]。注意しなければならないのは、IHEはDICOMやHL7のような規格そのものではないことである。いわば、規格の利用方法指南書に位置づけられる。

2.2.8 IHE のプロセス

表2-6にIHEのプロセスをまとめる。システム構築にあたって、ユーザが容易に（手間隙をかけずに）適切なベンダ選定を望む場合、IHEテクニカルフレームワークを要求仕様書（RFP）にすることが重要である。コネクタソンと呼ばれる接続試験は、このIHEテクニカルフレームワークを実装したことを確認する場であり、詳細は3.6章において解説される。

表 2-6 IHE のプロセス

共通シナリオの作成
→ 統合プロファイルの作成
→ 処理機能ユニットの抽出(アクタの仕様)
→ トランザクションの記述（DICOM,HL7 などを用いて）
→ テクニカルフレームワーク（パブリックコメント版）の記述
→ 公開とパブリックコメントの募集
→ テクニカルフレームワーク（試験実装版）の発行
→ コネクタソンによる接続試験
→ デモンストレーション
→ 医療機関の RFP への反映

2.3 IHE プロファイルにより HIE を構築するには

IHEのXDSプロファイルにより、医療連携の骨格が成り立つことを2.2.5に概説

した。ただし、これだけでは、ひとつのシナリオは実現できるものの、医療連携(HIE)の全体は構築できない。まず挙げられるのは患者IDの統一である。実際には統一しなくとも､各医療機関の患者IDの対応(マッピング)が取れればよい。さらに、HIE構築には、セキュリティ確保、コミュニティの設立に関する様々な規定、コミュニティを超えるアクセス、などの課題があり、それぞれの統合プロファイルによる対応が進んでいる。

2.3.1　患者 ID の統合

図2-4に、施設ごとに異なる患者IDを相互に参照するIHEの方法を示す。この場合のアクタは、患者IDソース(提供機能)、患者ID相互参照マネージャ、患者IDコンシューマ(利用者)の３つである。患者IDは、各医療機関の患者IDソースによって中央にある患者ID相互参照マネージャに登録する（患者ID提供）。マネージャは、各医療機関からの患者IDの対応付け（マッピング）を行なっておく、同時にドキュメントレジストリに患者IDを提供しておく。

医療情報にアクセスしたい各医療機関は、患者IDコンシューマ･アクタを使っては患者ID相互参照マネージャに問い合わせる。結果、自病院の患者IDが医療連携するコミュニティ全体の中のID（グローバルID）を知ることができる。ドキュメント・レジストリは、グローバルIDの患者IDを提供するソースから入手する。

このプロファイルは、患者ID相互参照・統合プロファイル（PIX:Patient ID Cross Referencing:）と呼ばれる。また、患者名、生年月日などの基本情報から、患者IDを知ることのできる統合プロファイル(PDQ：Patient Demographic Query)も利用することができる。

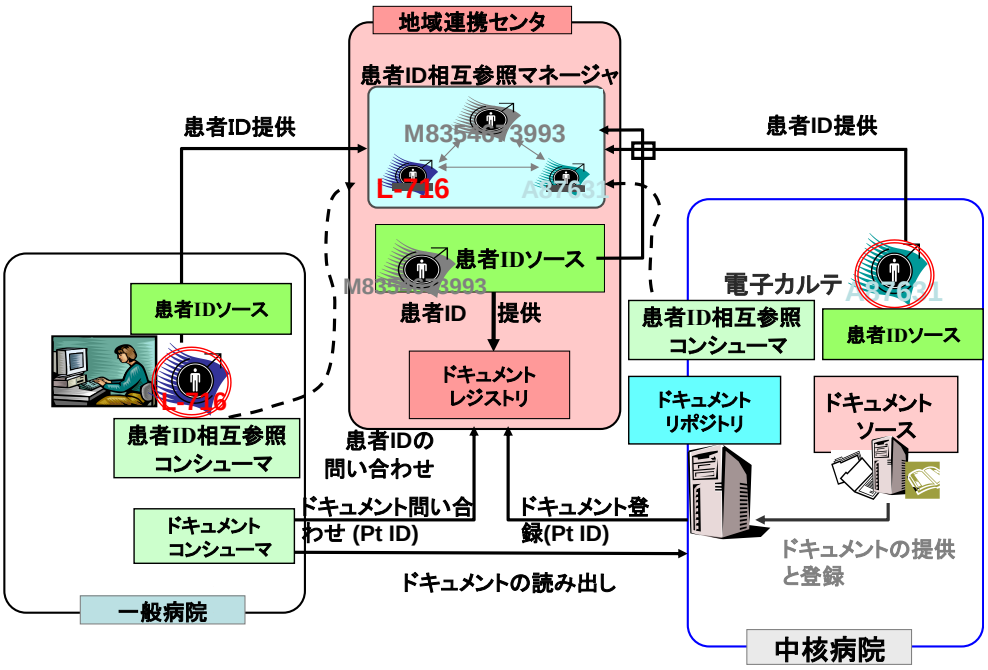


図 2-4　患者 ID の相互参照

2.3.2　連携基盤

表2-1にIHEによる連携のプロファイル名を掲げた。XDSはレジストリ、リポジトリという仕組みで共有することを目指しているのに対して、1対１（ポイントツウポイント）の通信で相手にドキュメントを提供するXDR（Cross Enterprise Document Reliable interchange）や可搬媒体によってドキュメントを届ける仕組みXDM（Cross enterprise Document Media interchange）などもIHEでプロファイルとして記述されている。特に後者はすでに述べたように大変簡便な共有基盤となる。XDMは、XDSのドキュメントをそのまま保つことになっている。さらに画像ファイルの簡単な媒体交換方法として、PDI（Portable Data for Imaging）プロファイルも用意されている。PDIの仕様の中に診療情報提供書などを含むことも可能であり、すでに利用が始まっている。

情報共有の基盤をIHEで実現する方法を解説してきているが、情報交換型の基盤として構築を進め、段階的に基盤を強化し、情報共有型へ移行していく方法もIHEを利用することで可能である。特にXDR,XDMの各統合プロファイルはファイルのフォーマットはXDSと同じものを用いているので、補完して利用することができる。

2.3.3　連携コンテンツ

XDS、XDR、XDMは、ドキュメントを連携する仕組み、あるいは基盤と呼べるものであるが、実際に共有するドキュメントの内容については、別の統合プロ

ファイルで定義されている。簡便のためコード名だけで掲げると、画像共有の場合はXDS-I、退院時サマリの共有はXDS-MS、臨床検査共有はXD-LAB、患者個人医療情報共有XPHR、救急部門ではEDRなどがある（表2-7）。これらのドキュメントの定義を行うプロファイルは、順次、様々な領域で開発が進んでいる。

表 2-7 コンテンツ統合プロファイル

統合プロファイル略称	統合プロファイル名	取り扱う情報
XDS-I	cross enterprise Document Sharing for Imaging	画像情報
XDS-MS	cross enterprise Document Sharing of Medical Summaries	退院サマリ情報
XD-LAB	Sharing Laboratory reports	臨床検査情報
XPHR	eXchange of Personal Health Record Content	個人医療情報
EDR	Emergency Department Referral	救急部門情報

2.3.4 セキュリティ対策と施設における運用方法

実際にインターネットを用いて相手に情報を送り届けるには、セキュリティの確保が要求される。例えば、正しいユーザかどうかは、PWP（職員の登録簿）、ユーザ認証については、XUA、アクタ間での相手認証は、ATNA（監査証跡とノード認証）、誰がアクセスしたかの監査証跡は、ATNA、改ざんはないかについて、データ完全性には、CT(時刻の整合）,及びATNA, あるいは、DSG(ディジタル署名）が用いられ、データ秘匿（暗号化）については、ATNAなどの統合プロファイルが利用可能である。アクセス制御については、Whitepaper（統合プロファイル策定に向けての議論がまとめられている）の形で解説されている。以上を表2-8にまとめる。セキュリティの各項目がどのように各統合プロファイルに関連するかは表2-9のとおりである。

表 2-8 セキュリティ関連統合プロファイル

セキュリティ対策	統合プロファイル名
ユーザ認証	職員の登録（PWP：Personnel White Pages）
	施設間ユーザ認証（XUA：Cross-Enterprise User Assertion）
アクタ（機器、ノード）認証	監査証跡とノード認証（ATNA ：Audit Trail and Node Authentication）
アクセス制御	Access Control(White papers)
監査証跡	ATNA
データ完全性	CT(時刻の整合）， ATNA(TLS：Trusted Layer Security オプション)
ディジタル署名	DSG(Digital Signatures)
データ秘匿	ATNA(TLS オプション)
プライバシ同意	BPPC(Basic Patient Privacy Consents)
ドキュメントの利用可能通知	NAV(Notification of Document Availability)

表 2-9　セキュリティ関連の統合プロファイル

○:直接的に関係 △:間接的に関係	説明責任	認証	アクセス	秘匿	完全性	否認拒否	個人情報保護	利用性
ATNA(監査証跡とノード認証)	○	○	○	○	○	○	○	
BPPC(患者同意)				△			○	
CT〔時刻の整合性)	○	△				○		
EUA(施設内ユーザ認証)	△	○	△	△		△	△	
XUA(施設間ユーザ認証)	△	○	△	△		△	△	
DSG(電子署名)	○	○			○	○		
XDS				○	○		△	○
XDR				○	○		△	○
XDM			△	○	○		△	○
PWP(職員の台帳)	△	○	○			△		

2.3.5　コミュニティ(XAD)の設立

コミュニティの設立方法についてもIHEではテンプレートとして記述がなされている(表2-10)。例えば、組織規程、運用規程、会員規程、ドメイン外との接続性、システム仕様、メタデータ、セキュリティ技術などである。IHEでは、これらは、統合プロファイルではなく、White Paperという形で説明がなされているので利用することができる。これについては第4章で詳述される。

表 2-10　コミュニティ設立に必要な事項

1. 組織規程
（構成、設立者、運営者、経済的、税務的検討、透明性、責任機関、法的事項の管理、債務、免責事項）
2. 運用規程
（サービス契約、日常管理、トラブル、メンテナンス（追加、更新、バックアップ)、災害復旧）
3. 会員規程
4. ドメイン外との接続性
5. システム仕様
（レジストリ、リポジトリ、ソース、コンシューマ、患者 ID 相互参照マネージャ、監査証跡リポジトリ、ドメイン間トランザクション）
6. メタデータ　(辞書)
7. 患者同意
8. セキュリティ技術
（承認、認証、アクセス、完全性、倫理、監査証跡、リスク解析）

2.3.6　コミュニティを超えた連携

連携を行うコミュニティが増えていくと、やがては、コミュニティを超えた共有も視野に入れる必要がある。IHEはそれに対しても統合プロファイルを用意している（XCA：Cross Community Access）。その仕組みは、図2-5にあるように各コミュニティの情報の連携を担当するアクタを用意し、そのアクタを通じてのみ連携ができるような構造とすることである。コミュニティへの入出力を担当するアクタをゲートウェイ（Gateway）アクタと呼ぶ。各コミュニティのコンシューマの要求を外部に問い合わせるアクタを「開始ゲートウェイ（Initiating Gate Way）」として定義し、このアクタから外部にあるコミュニティが問い合わせに応じるアクタ「応答ゲートウェイ（Responding Gate Way）」を用意して通信を行う。開始ゲートウェイが応答ゲートウェイに問い合わせを順次行っていって、情報を探す仕組みである。通信を可能とするにはコミュニティ間でのポリシーが合意されていることが必要であるなど、いくつかの前提条件（共通の用語を採用していることなど）が必要であるが、技術的な枠組みとして可能な状況となっている。

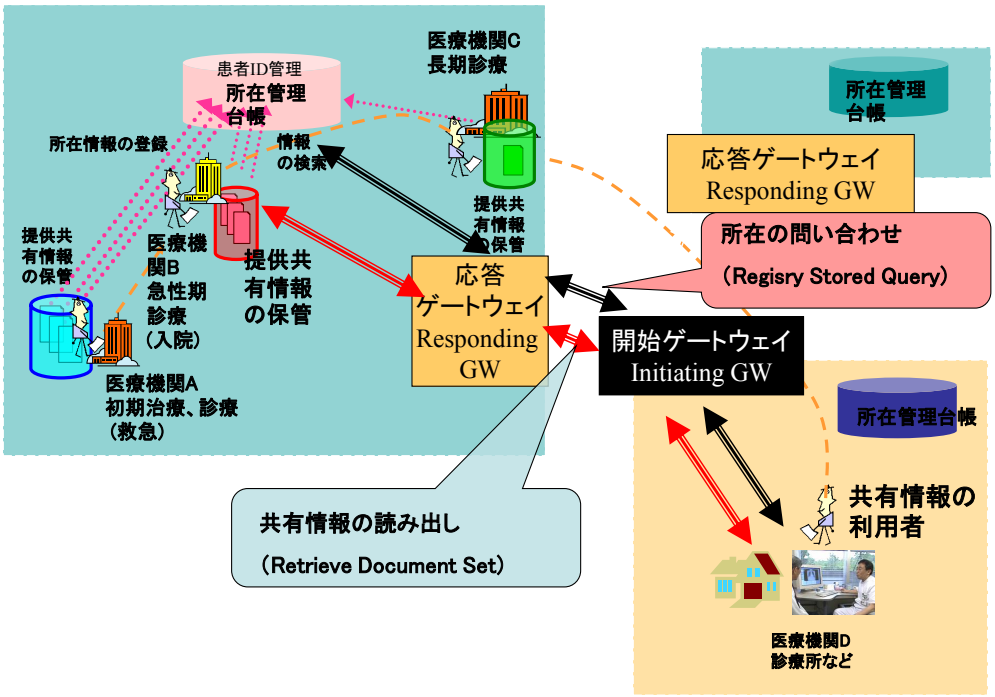


図 2-5　コミュニティ間の情報共有

2.4　構築手順と要求仕様

表2-11にHIEの構築手順と関連するプロファイルをまとめた。コミュニティの確立が合意されると、XDSの構築に向けて要求仕様書を作成する。共有するコン

テンツの内容、範囲を決定する。患者ID共有基盤の設計、セキュリティ確保のための基盤設計を行う。全体の運用としては、セキュリティ確保が医療情報システムの安全管理ガイドラインを満足していることが求められる。IHEによる構築では用いられる技術の仕様が標準となっており、安全管理ガイドライン適合の検討が容易に進められることになる。これについては次節に述べる。XADとしての確立に向けて、運用体制を構築することが重要であり、IHEはそのためのガイドラインも提供している。

具体的な要求仕様書の作成については第3章に、準備の手順については附属書Fに、それぞれ詳述される。ベンダに対する提案要求事項については附属書Gにまとめた。

表 2-11 IHE による連携システムの構築手順

1. コミュニティ（XAD）の確立：
   Handbook ： Template for XDS Affinity Domain Deployment Planning
2. XDS の構築(要求仕様書の作成)；XDS
3. コンテンツの決定(要求仕様書の作成)：XDS MS
4. 患者 ID 共有基盤(要求仕様書の作成)： PIX,PDQ
5. セキュリティの確保(要求仕様の作成)：
   ATNA,CT,XUA,PWP,DSG,Handbook(HIE Security and Privacy through IHE Profiles, Preparing the IHE Profile Security Section)
6. 安全管理ガイドラインへの適合検討　運用管理規程の作成
7. XAD の運用

2.5 安全管理ガイドラインと HIE

わが国におけるHIE運用においては、平成14 年に厚生労働省より出された通知された「外部保存通知」に対応するために整備された「医療情報システムの安全管理に関するガイドライン（以下、安全管理ガイドラインと略す。2010年第4.1版が出されている)」（厚生労働省）を満足していることが求められる。それと同時に、医療情報を受託管理する情報処理事業者向けガイドラインや、ASP・SaaS（Software as a Service:ネットワークを通じて、アプリケーション・ソフトウェア及びそれに付随するサービスを利用させること）型の事業者向けのガイドラインも相次いで整備されている(表2-12)。

表 2-12　HIE に関連するガイドライン

1. 医療情報システムの安全管理ガイドライン（2010 年 4.1 版：厚労省）
2. SaaS 向け SLA（Service Level Agreement）ガイドライン（2008 年：経産省）
3. ASP・SaaS における情報セキュリティ対策ガイドライン(2008 年：総務省)
4. 医療情報を受託管理する情報処理事業者向けガイドライン（2008 年：経産省）
5. ASP・SaaS 事業者が医療情報を 取り扱う際の安全管理に関するガイドライン（2009 年：総務省）

安全管理ガイドラインは、外部保存にあたって、ネットワーク上でのオブジ

ェクトセキュリティとチャネルセキュリティの対策、送り手、回線事業者、ネットワークサービス提供者、受け手の間で責任の空白をつくらないよう、責任分界点の明確化を要請している。HIEはガイドラインにおける外部保存の考え方と同等と考えるべきであり、レジストリのサービス事業者に対しては「委託」となり、リポジトリによる情報共有については、「共同利用」という形を取ることが可能であるが、患者の同意を得て「第三者提供」とならざるをえない場合もある。

XADを運用する仕組み全体をSaaSとみなすことができれば、ビジネスとして運用する側と、利用する側の関係が明確になる。XADのモデル例を図2-6に掲げた。点線で囲まれた部分をひとつのサービスとして事業者が提供することを想定すると（ただし、レジストリとリポジトリは別々の場所にあることを前提とする）、医療情報連携サービスシステムとしてSaaSの形態となると考えられる。サービス事業者は所在情報を預かるが、共有する医療情報は各医療機関がリポジトリとして所有する形をとる。このサービスによりXAD内の医療機関が互いに医療情報を参照することができる。

以上、ガイドラインとHIEについては、第4章にて詳述される。

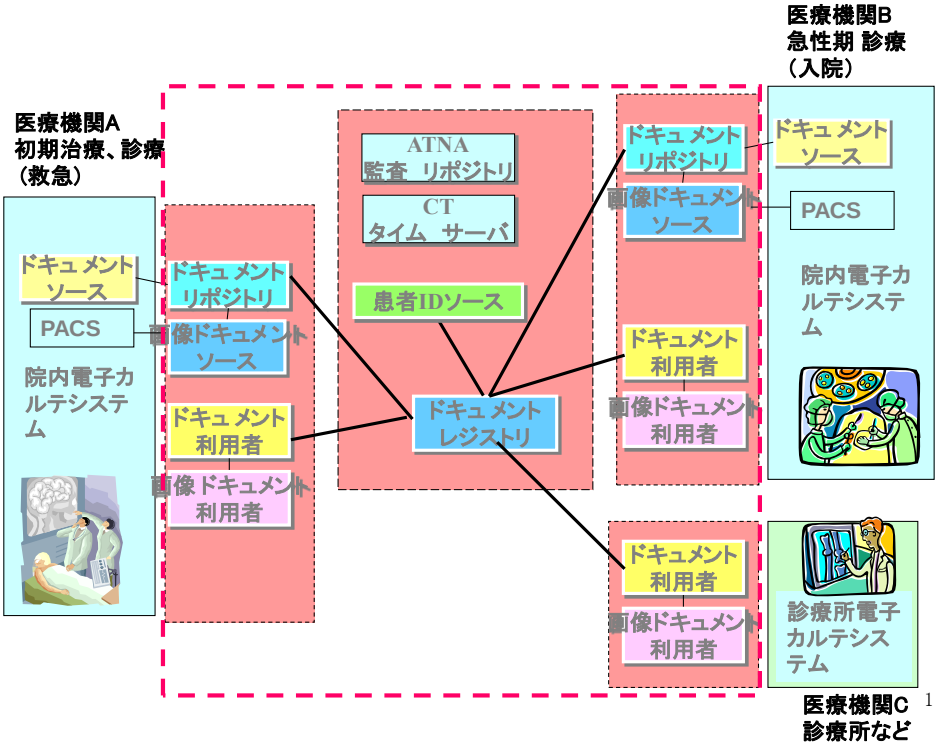


図 2-6　IHE による HIE の構成

2.6　IHE のめざすもの

IHEは様々な領域(放射線、循環器、眼科、治療、ITインフラ、検査デバイス、病理、内視鏡、患者ケアなど)で統合プロファイルの開発が行われている。これらは、医療機関内での情報化を目的としているものと医療機関を結んだ情報化

を目指すものに分かれる。ここでは、医療機関連携（HIE）のシナリオを例として取り上げて解説してきたが、医療機関内の情報とのリンクは極めて重要であり、そこにおいても医療機関内の種々のプロファイルの利用がIHEで可能である。以上、IHEによれば、表2-13のごとくHIEの要素が実現できることが明らかになり、IHEによるHIE構築、即ち共有された電子カルテシステム構築ができることになる。

表 2-13　IHE によってできること

1. 連携の仕組み（基盤）を確立でき、標準化された情報（コンテンツ）の利用が可能である。
2. 患者 ID の相互参照が可能となり、情報共有ができる。
3. 運用に当たって、IHE はセキュアな基盤を確保する統合プロファイルを供給できる。
4. コミュニティの設立･運営のガイドラインが用意されている。
5. コミュニティを超えて広域に共有を展開する仕組みができている。
6. 医療機関内の電子カルテなどの情報システムとの接続が可能である。

海外においては、地域ごとのHIEの構築が展開されている（RHIO:Regional Health Information Organizationと呼ばれる）。わが国においても、2007年より3年間実施された名古屋プロジェクトにおいてXDSを中心とした脳卒中医療連携が行われている。詳細は第３章において紹介する。

わが国におけるIHEの動きは、2001年よりIHE-J委員会として開始された。2007年には、法人として日本IHE協会が設立され、国際的なIHEの動きと連携した必要な統合プロファイルの開発や、既存のプロファイルの国内拡張と国際整合、コネクタソンの実施、などを行っている[4]。2007年から厚生労働省より「医療情報システムの相互運用性確保のための対向試験ツール開発事業」を受託し、コネクタソンを効率的に実施するためのツール開発を続けている。

参考文献

[1] 地域連携クリティカルパスと疾病ケアマネジメント　日本疾病管理研究会　中央法規出版　2009 年 4 月

[2] 地域医療連携実践ガイドブック　治療 2008 年 3 月増刊号　南山堂

[3] http://www.ihe.net

[4] http://www.ihe-j.org

[5] IHE 入門　篠原出版新社　東京　2005

[6] IHE 超入門　篠原出版新社　東京　2008

3.　システム構築の要求仕様

本章では、IHE による地域医療連携情報システムの構築に際して、要求仕様のまとめ方について解説する。また、地域連携パスの事例をもとに、具体的な要求仕様を例示する。要求仕様は、目的のシステムで必要とする機能およびその要件をまとめたものである。

本章に関連して附属書 A では、施設間連携での画像共有の事例を紹介する。主な IHE 統合プロファイルについては、附属書 B～D で詳細に解説する。また、実装技術に関しては、附属書 E で具体的なオープンソースの利用方法を紹介する。

なお、本章の内容の一部は、平成 18～20 年度経済産業省委託事業「地域医療情報連携システムの標準化及び実証事業」（東海ネット医療フォーラム・NPO[代表理事及び事業の統括責任者：名古屋大学名誉教授吉田純]）の成果をもとにしている。詳細は、下記のサイトを参照。

注)・JAHIS：地域医療情報連携システム関連ドキュメント
http://www.jahis.jp/tiikirenkei_pj/tiikirenkei_top.html
・東海ネット医療フォーラム・NPO：関連ドキュメント
http://www.medinet-tokai.com/npo/index.html

3.1　構築システムの例

厚生労働省では、医療施設体系のあり方に関する検討会等で、我が国の医療提供体制をめぐる様々な課題をとりあげ、医療施設の体系、地域における医療連携等のありかたに関する検討が重ねられている。特に、下記の課題については、実現性のある標準的な方式の確立が強く求められている。

・地域連携パスへの取り組み
・医療介護福祉連携、特に退院調整機能、退院時支援機能の構築

そのためには、体制整備とともに、医療機関等のネットワーク化や電子的情報の安全で円滑な交換・共有等の IT 基盤の整備を進めていく必要がある。

3.1.1　ユースケースシナリオの作成

システム構築にあたっては、まず、目標の支援システムが、どのような環境で、どのように使用されるかを決める必要がある。一般的に、地域医療連携では、さまざまな業務場面があり、想定するシナリオも多様である。しかし、医療施設間の情報共有に焦点を絞ったユースケースを考えることにより、地域医療連携情報システムとして必要な事柄を浮き彫りにすることができる。

（１）XAD アフィニティドメイン

ここでは、２次医療圏での脳卒中や大腿骨頸部骨折などの地域連携パスでの情報共有の場面を想定する。急性期病院は、５施設、回復期リハビリ病院は、

２０施設、維持期は、診療所や介護ステーションなど１００施設程度の連携を考える（規模は、実情に応じて縮小、拡張が可能）。図 3-1 は、ここで想定する地域連携パスの XAD アフィニティドメインの構成例である。急性期 A、回復期 B、維持期 C で表された施設は、自施設内にリポジトリを持つドメインを示している。一方、病院、診療所、リハビリ病院などに設置した連携クライアントは、自施設内では、リポジトリを管理せず、他の施設にリポジトリがあることを表している。

これらの参加施設が、共通のポリシーで連携する XAD アフィニティドメインとなりコミュニティを形成する。

主に、急性期病院、リハビリ病院、かかりつけ医等との連携が、地域医療センタに設置するレジストリなどを介して行われるものとする。

連携に必要な診療情報は、患者の同意を得て、レジストリに登録される。それらの情報のありか（所在）情報をもとに、登録された診療情報にアクセスが可能となる。

患者の症状、治療経過に従って、適切な連携パスが選択され、リハビリ情報などのフィードバック（治療結果報告）を情報共有し、患者ごとに適切な治療が提供される。

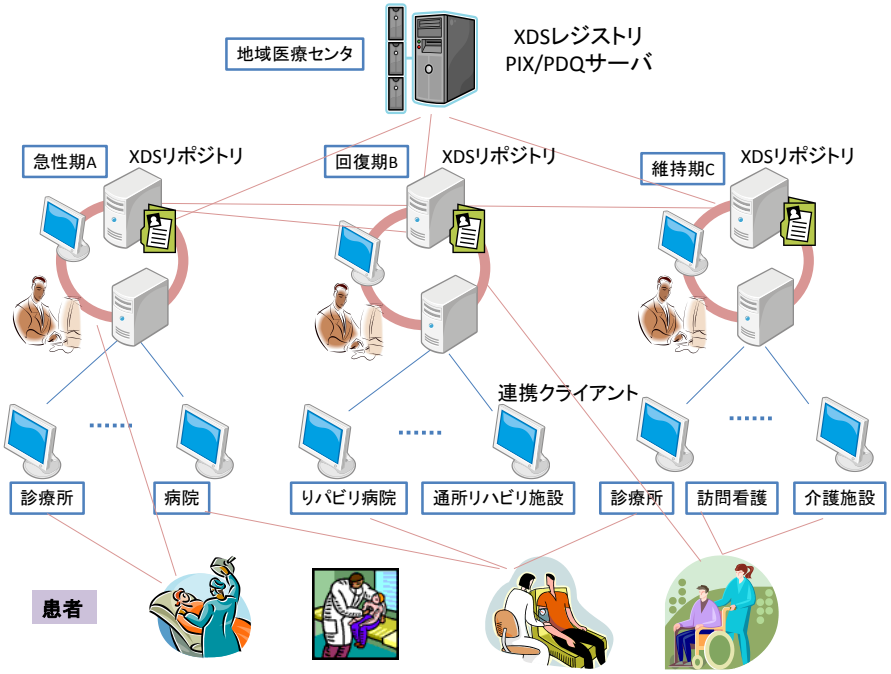


図 3-1 地域連携パスの XAD アフィニティドメイン

（２）シナリオ

ここでは、図 3-2 に示すような、医療機関 A（送付元）、医療機関 B（送付先）の施設間で、連携パス情報を共有する場面のシナリオを例示する。地域医療センタに設置する PIX マネジャは、患者 ID の管理を行い、レジストリは、患者ごとに、目的に応じたフォルダを用意し、関連するドキュメントのありか情報（リ

ポジトリの場所）などのメタデータを登録、管理する。

想定される地域連携パスの支援システムの処理の流れは、以下のとおりである。

① 患者 ID の登録
新規の患者については、患者基本情報を施設患者 ID とともに、PIX に登録する。患者には、XAD 内で管理される共通の患者 ID を発行する。

② 診療情報の登録
作成した診療情報（CDA ドキュメント、参照する画像ファイル、添付する検査データなど）を、電子署名をつけて、その患者専用の XDS のフォルダに入れる（登録する）。

③ アクセス権の設定
作成した送付先（施設リスト、利用者リストから選択）を決定し、アクセス権を設定する。

④ 送付先への通知
診療情報を登録したことを、送付先に通知メッセージで知らせる。

⑤ 通知メッセージの受信
送付元からの通知メッセージを受信する。

⑥ 診療情報の受取り
ドキュメントの送付の通知を確認した後、そのドキュメントを XDS レジストリ、リポジトリから取得する。

⑦ 受取りを送付元に返信
フォルダに格納された診療情報を、検索、取得し確認後、受取りメッセージを送付元に送信する。

⑧ 受取りメッセージを受信
送付したドキュメントを相手が参照したことを示す受取りの返信メッセージ（受取りメッセージ）を受信する。

⑨ アクセス権の変更
受取りメッセージを確認した後、必要ならば外部からのアクセスができないようにする。

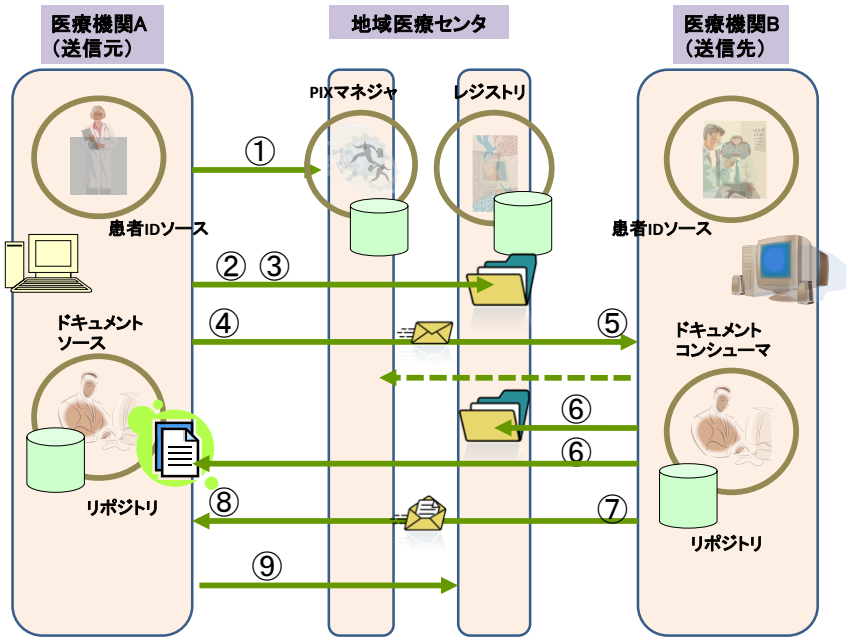


図 3-2 地域連携パスのシナリオ

3.1.2 地域連携パスの支援システムに必要な機能

作成した地域連携パスのシナリオの業務を支援するシステムに必要な主な機能とその要件をまとめると以下のようになる。

（1）患者 ID 管理機能

患者の氏名や住所、性別や生年月日などの基本情報及び各施設で管理されている患者 ID などを登録し、新規登録時には XAD アフィニティドメインで一意なグローバル ID を発行できること、また、患者の属性で、患者情報を検索できる。

（2）情報共有機能

ドキュメント登録（共有情報のリポジトリへの格納、メタ情報のレジストリへの登録）、検索、取得する機能が必要である。さらに、連携パスの情報を表示（対象の患者ごとに、連携パスと、関連情報のありかを表示）でき、ドキュメント取込（共有情報の取込）ができる。

（3）コンテンツ仕様

共有する情報（コンテンツ）は、目的ごとに多様である。連携パスでは、それらのコンテンツの内容を機械的に処理、分析することで、さまざまな支援機能を提供できるようになる。それらのコンテンツの仕様を標準化することが重要であり、低コストで効果的なシステム開発には必須である。

（4）利用者・施設管理機能

多施設、多職種の連携システムでは、セキュリティに配慮した情報共有を達

成するため、施設、利用者、システム（ノード）の利用者に関する情報を適切に登録管理できる機能が必要である。

（５）シングルサインオン（SSO）機能

施設間にまたがる利用者の認証、および提供される地域連携支援サービス間のシングルサインオンによる連携機能が必要である。具体的には、利用者・施設管理をもとに利用者の認証を行い、登録利用者であれば認証済みのチケット（トークン）等を発行する機能を持ち、また、それぞれの支援サービスを利用できるか判定する機能を提供するなどの機能が必要である。

（６）通知機能

相互のコミュニケーションを支援する通知機能が必要である。以下のような通知メッセージをやりとりする。

・開示通知（アクセス権者へ開示する）
・受取通知（開示された共有情報の取込を通知）
・通知メッセージ受取り（開示通知、受取通知の受取り）
・受取通知（共有情報の受取りを通知）

（７）アクセス制御機能

特定の患者の診療情報を治療関係者の利用者が閲覧できるようにするため、その情報のアクセス権取得者（アクセス許可を受けた関係者）を明確にし、アクセス権取得者のみが、その情報を取得できるようなアクセス制御機能が必要である。同時に、アクセス権取得者の登録（紹介先の施設、医師などを通知先として追加登録）の機能も必要である。

（８）監査証跡機能

患者の基本情報、診療情報は、機微な個人情報であり、それらを保護することが重要である。セキュリティ要求事項の中でも、監査証跡のログを取ることが、不正なアクセスを予防する上からも求められている。利用者によって実行された機能（記録作成、アクセス、更新、その等）と、それが実施された日時を識別できる記録をとる機能が必要である。

3.2　関連する統合プロファイルの機能と利用判断

地域連携システムを構築には、相互運用性を確保するために、標準的な共通の基盤の上に展開することが重要である。ここでは、必要な基盤となる機能要素に対して、IHE の技術（文書）が、どう対応するかを示し、そのまま利用可能な技術と、さらに追加することが望まれる機能について述べる。

3.2.1　IHE の技術（文書）との対応

3.1.2 で述べた「地域連携パスの支援システムに必要な機能」について、それぞれの機能に対応する IHE の技術（文書）は、表 3-1 のとおりである。また、図 3-3 は、必要な主な機能と IHE の関連技術を図示したものである。

IHE の ITI 統合プロファイルは、毎年更新され、2009 年には第 6 版が発行されている。HL7 や OASIS などの標準化の進捗や関連技術の進歩、実装経験などをもとに、改良が重ねられ進化してきている。

地域医療連携情報システムの中核となる PIX/PDQ、XDS、ATNA の部分の技術（文書）は安定したレベルになっている（3.3～3.5 参照）。しかし、全体を通じてまだ検討段階にあるものもあり、適用には、追加の設計が必要になる部分もある。

また、コンテンツの仕様については、現時点では国内の標準が決められておらず、別途検討が必要である。

表 3-1 IHE の技術（文書）との対応

	項目	対応するIHEの技術（文書）
1	患者ID管理機能	・Patient Identifier Cross-Referencing (PIX) ・Patient Demographics Query (PDQ) ＜HL7V3対応版＞ ・Patient Identifier Cross-Reference (PIX) and Patient Demographic Query (PDQ) HL7 v3
2	情報共有機能	・Cross-Enterprise Document Sharing - b (XDS.b) ・Cross-Enterprise Document Sharing for Imaging (XDS-I.b) ＜旧版＞ ・Cross-Enterprise Document Sharing (XDS) ・Cross-enterprise Document Sharing for Imaging (XDS-I) ＜特定用途＞ ・Cross-Enterprise Document Reliable Interchange (XDR) ・Cross-Enterprise Document Media Interchange (XDM) ・Portable Data for Imaging (PDI)
3	コンテンツ仕様	・Cross Enterprise Sharing of Medical Summaries Integration Profile (XDS-MS) ・Emergency Department Referral (EDR) ・Exchange of Personal Health Record Content (XPHR) ・CDA Content Modules ＜特定用途＞ ・Portable Data for Imaging (PDI)
4	利用者・施設管理機能	・Personnel White Pages (PWP) ＜施設内向け＞ ・Enterprise User Authentication (EUA)
5	シングルサインオン（SSO）機能	・Cross-Enterprise User Authentication (XUA) ＜施設内向け＞ ・Enterprise User Authentication (EUA) ＜技術白書＞ ・Access Control
6	通知機能	・Notification of Document Availability (NAV) ＜技術白書＞ ・Publish/Subscribe Infrastructure for XDS.b
7	アクセス制御機能	・Basic Patient Privacy Consents (BPPC) ＜技術白書＞ ・Access Control
8	監査証跡機能	・Audit trail and Node Authentication (ATNA) ・Consistent Time (CT)

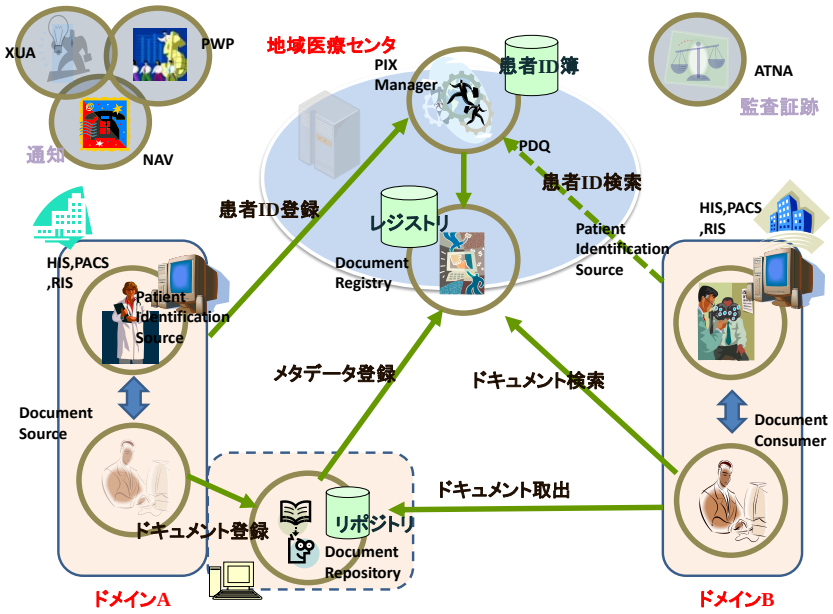


図 3-3 必要な主な機能と IHE の関連技術

3.2.2　追加することが望まれる機能とその要件

IHE の技術文書では、地域連携支援システムの構築に必要な機能要素は、カバーしているが、それらの個々の機能を統合して全体で整合性のあるシステムとして組み上げる方式については、まだ、技術白書のレベルで検討が続いている段階である。

実際の連携システムの構築においては、IHE の技術文書で示された方式などを参考にして、さらなる追加の機能設計が必要になる。具体的には、以下の機能が有機的に連動して動作する環境を実現する必要がある。

・フォルダ機能
・利用者・施設管理機能
・シングルサインオン（SSO）機能
・アクセス制御機能
・通知機能

ここでは、名古屋プロジェクトでの実装例を詳細化の一例として示し、それらの要件をまとめる。

（1）フォルダ機能

フォルダ機能は、XDS の仕様として定義されている。しかし、その利用の仕方や管理の仕方については、さまざまな方式が考えられ、統一性を持たせる必要がある。

- 各フォルダは、患者ごと、目的（疾患別の連携パスなど）ごとに設ける。
- フォルダ単位で、アクセス権を制御できるようにする。

- 診療情報のメタ情報は、すべての登録利用者がアクセスできる。
- 診療情報の本体（CDA など）に、アクセスできる登録利用者は、フォルダごとに管理する。
- フォルダは、最初に、そのフォルダを作成した登録利用者が、所有者(owner)となる。

（２）利用者･施設管理機能

利用者及び施設の登録管理は、アクセス制御、通知機能、シングルサインオン、監査証跡などのセキュリティに関連した機能を実現するのに必須である。IHE では、利用者の登録管理機能として LDAP（Lightweight Directory Access Protocol）をベースにした職員録（PWP）仕様が提示されている。しかし、LDAP v3 は利用者が登録や離脱を、自ら自由に行えるような Web サービスの利用者管理には向いているが、医療の地域連携のように厳格に利用者管理を行う必要がある場合には、異なる方式も検討すべきである。そのような観点から、レジストリの機能（ebXML の ebRIM3.0 および ebRS3.0）を利用し利用者･施設の情報を登録することで、サーバ側のアプリケーションからマスタ情報として参照できるような方式を実現した。実装した主な利用者･施設管理機能の要件は、以下のとおりである。

- 利用者及び施設の加入、離脱などの状況変化に対応できる。
- 多施設、多職種の連携に必要な情報共有及びコミュニケーションを支援できる。
- アクセス制御に必要な職種、グループなどの情報を登録管理できる。
- 通知機能の実現に必要な利用者情報を登録管理できる。
- シングルサインオンに必要な、ID 認証、パスワードなどの情報を登録管理できる。
- 監査証跡のログ中で、利用者を識別するための情報を登録管理できる。

（３）シングルサインオン機能

IHE では、EUA (Enterprise User Authentication)でシングルサインオンの機能を提供している。それらは、主に施設内での利用者管理をベースにしたものである。一方、施設間では、XUA (Cross-Enterprise User Authentication)が、同様の利用者の認証機能を定義している。XUA では、シングルサインオンについては、十分な言及はなされていないが、技術白書「Access Control」には、最新の Web 技術をベースにしたシングルサインオンの導入、適用について検討がなされている。実装した主なシングルサインオン機能の要件は、以下のとおりである。

- 利用者･施設管理機能と連携して ID、パスワードで利用者認証を行える。
- アプリケーションからの要請で、利用者の認証を行いチケット(トークン)を発行する。
- アプリケーションから提示されるチケットの有効性を判断する。

（４）アクセス制御機能

多施設、多職種による地域連携では、アクセス権の管理が、運用上重要な問題になる。技術的には、個別にアクセス権付与ポリシを設定できるようにし、それらに従ったアクセス制御が可能であるが、それらを、安全にかつ簡易に運用できるようにするには、より大がかりなシステムが必要となる（IHE の BPPC および Access Control 参照)。

以下は、同様のアクセス制御の基盤技術を用いて単純化した方式を実現したもので、フォルダをベースにしたアクセスポリシの例である。

- 加入者リストは、診療情報にアクセスする権限をもつ加入者（利用者）を保持する。
- 各フォルダに、加入者リストを関連づける。
- 加入者リストに、登録利用者を、追加、削除することができる。
- 加入者は、新規の登録利用者を追加する権限をもつことができる。
- 管理者のみが、登録利用者を削除することができる。
- 加入者リストの更新（加入者リストの新規登録、利用者の登録、削除）時に、アクセス制御ポリシー（ACP）を更新することができる。
- アクセス制御は、利用者のロールに基づき行うことができる。
- アクセス制御の対象は、対象フォルダに所属するドキュメントエントリ（メタデータ全体）とすることができる。

（５）通知機能

IHE では、ドキュメントの登録などを通知する機能として、SMTP を用いた電子メールによる通知機能を定義している。しかし、地域連機を支援する機能としては、それだけでは十分とは言えない。特に、電子メールを利用する場合には、暗号化などセキュリティを考慮する必要がある。以下は、実装した主な拡張した通知機能の要件の例を示す。これらは、技術的には、IHE の技術白書「Publish/Subscribe Infrastructure for XDS.b」の応用となっている。

- 加入者リストから、必要に応じて通知者を選択（制限）して、情報共有、連携のための情報（メッセージ）を通知することができる。
- メッセージを登録することで、送信先に通知できる。
- 用途別にメッセージにタイプを指定できる。
- 登録したドキュメントの ID を通知できる。
- メッセージの送付先として、グループ指定ができる。
- 通知のタイプを設けることができる。
- 送信するテキストの内容は、通知のタイプごとに、アプリケーション側で定めることができる。
- Web サービス及び電子メールの両方を組み合わせた手段で通知ができる。

3.3 XDS 関連機能とその要件

この節では、XDS 及び XDS-I に関する機能要件を示す。なお、実際の地域連携システム等に適用する場合は、それぞれの目的によって要求仕様は異なる。また、IHE の最新仕様などを確認して決定する必要があり、ここでは、要求定義の例を示す。

XDS（Cross-Enterprise Document Sharing）は、施設間で共有する医療ドキュメントを、互いの施設から参照可能なリポジトリに格納し、各ドキュメントのありか情報をレジストリに登録する。施設間でドキュメントの交換が必要になった際に、レジストリを検索することで、該当するドキュメントが格納されているリポジトリを見つけ、そこからドキュメントを取り出し参照することができる。

初期の IHE の XDS 統合プロファイルは、ebXML の旧バージョン（ebRIM2.0 および ebRS2.0)に基づいて作成されたが、2007 年 8 月に、ebRIM3.0 および ebRS3.0 規格に基づいた XDS.b に改定された。XDS.b では、通信プロトコルが SOAP with attachment から、MTOM や MTOM/XOP などの新しい方式に変更になった。

注）MTOM：　Message Transaction Optimization Mechanism
　　XOP：　XML-binary　Optimized Packaging

図 3-4 は、施設間の文書共有プロファイル XDS.b に直接関与している各 IHE アクタのトランザクションを図示している。なお、機能の詳細は、附属書 B で解説する。

図 3-5 は、画像の施設間の文書共有プロファイル XDS-I.b に直接関与している各 IHE アクタのトランザクションを図示している。DICOM 画像の格納と登録、参照の方式を図示したものである。PACS に格納された画像データを、他施設から参照できるようにするため、その参照情報などを含む Manifest を作成し、それらをドキュメントリポジトリおよびドキュメントレジストリに登録する。コンシューマ側からは、まず Manifest を検索、取得したのち、その Manifest の情報をもとに画像データを取得する。

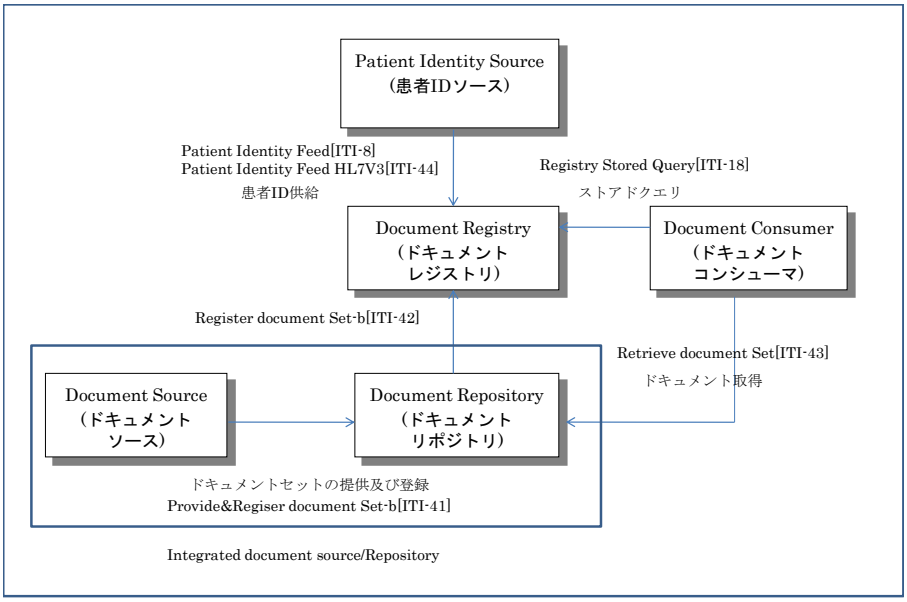


図 3-4　XDS.b の IHE アクタおよびトランザクション関連図

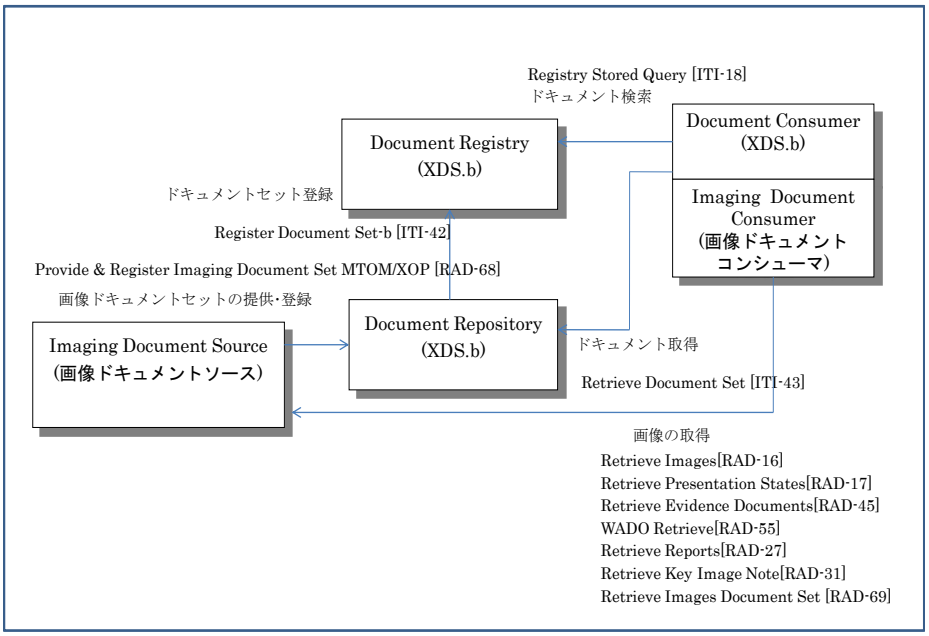


図 3-5 XDS-I.b の IHE アクタおよびトランザクション関連図

3.3.1 レジストリ機能

レジストリ機能（XDS.b 対応）に求められる要件は、以下のとおりである。

① ebRIM3.0 および ebRS3.0 規格に準拠した情報モデルを採用すること。
② ドキュメントリポジトリからのドキュメントセットの登録に対応すること。
③ ドキュメントコンシューマ、画像ドキュメントコンシューマからの問い合わせに応答すること。問い合わせ言語については、ebRIM3.0 および ebRS3.0 の Registry Service によって指定された SQL 相当の問い合わせ式に対応すること。
④ 提出されたメタデータの検証機能を有する ebRIM3.0 および ebRS3.0 に対応した登録アダプタ機能を有すること。
⑤ この登録アダプタ機能は、ebRIM3.0 および ebRS3.0 レジストリ用のプリプロセッサとして機能し、レジストリ全体の一貫性を維持し、患者 ID、MIME タイプ、メタデータ、コード化された値および提出中のドキュメントエントリを検証すること。
⑥ 登録されるデータの各フォルダ属性の最終更新時間を維持管理する機能を有すること。
⑦ ドキュメントの追加および置換を管理する機能を有すること。

3.3.2 リポジトリ機能

リポジトリ機能（XDS.b 対応）に求められる要件は、以下のとおりである。

① ebRIM3.0 および ebRS3.0 規格に準拠した情報モデルを採用すること。
② ドキュメントソース、画像ドキュメントソースからのドキュメントセット登

録に対応すること。
③ 登録されたドキュメントセットは、永続的に管理可能な論理構造を有し、メタデータ（ドキュメントセットのインデックス情報）を Register Documents トランザクションによってドキュメントレジストリに登録する機能を有すること。
④ 本アクタが送信するメッセージは、ebRIM3.0 および ebRS3.0 メッセージ・フレームワークを使用し、MTOM や MTOM/XOP 形式の SOAP（Simple Object Access Protocol）メッセージであること。
⑤ ドキュメントコンシューマからのドキュメント読み出しに対応すること。

3.3.3 ドキュメントコンシューマ関連機能

（1）ドキュメントコンシューマ機能
ドキュメントコンシューマ機能（XDS.b 対応）に求められる要件は、以下のとおりである
① ドキュメントコンシューマからドキュメントレジストリを検索し、レジストリから返されるドキュメントエントリーリスト（リポジトリに存在する XDS ドキュメント所在および識別情報を含むメタデータからなる)を受信できる機能を有すること。
② 検索には、ebRIM3.0 および ebRS3.0 Registry Services によって指定された SQL 言語を使用可能であること。
③ PDF および TEXT 形式のレポートを表示する機能を有すること。
④ 参照ドキュメントをローカルディスクの任意のフォルダに任意のファイル名をつけて保存できる機能を有すること。

（2）画像ドキュメントコンシューマ機能
画像ドキュメントコンシューマ機能（XDS-I.b 対応）に求められる要件は、以下のとおりである。
① 画像ドキュメントコンシューマは、ドキュメントコンシューマを通じてドキュメントレジストリを検索し、レジストリから返されるドキュメントエントリーリストを受信できる機能を有すること。
② 入手した施設のドキュメントリポジトリにアクセスし、DICOM Manifest を入手する機能を有すること。
③ 入手した Manifest をもとに画像ドキュメントソースにアクセスし、WADO および DICOM 通信により画像を読み出す機能を有すること。
④ DICOM C-MOVE Service Class での読み出しが行なえること。
⑤ WADO 読み出しに対応すること。
注）DICOM：Digital Imaging and COmmunication in Medicine
WADO：Web Access to DICOM Persistent Objects

（3） WADO 呼び出しに対応した DICOM 画像ビューア機能
WADO 呼び出しに対応した DICOM 画像ビューア機能（XDS-I.b 対応）に求められる要件は、以下のとおりである。

① WADO によって呼び出された画像を表示する機能を有すること。
② 表示対象となった画像の患者基本情報が画面上に表示されること。
③ 表示対象が 1 検査であった場合には、画像表示ウィンドウが表示され、複数検査または検査が指定されていない情報が表示対象となった場合は検査リストウィンドウが表示される仕様となっていること。また、システム設定により、必ず検査リストウィンドウが表示できる設定変更が可能であること。
④ 指定されたキー画像を表示する機能を有すること。
⑤ プレゼンテーションステイツを表示できる機能を有すること。
⑥ PDF あるいは TEXT 形式のレポートを表示できること。
⑦ 表示画像をローカルディスクの任意フォルダに任意ファイル名にて保存できる機能を有すること。
⑧ 画像表示については以下の機能を満たすこと。
拡大／縮小、パン、マスキング、左右反転、回転、WW/WC 調整、比較表示、シネ表示、オーバレイ表示、ROI 測定など。

3.3.4 ドキュメントソース機能

ドキュメントソース機能（XDS.b 対応）に求められる要件は、以下のとおりである。
① ドキュメントソースからドキュメントリポジトリに、XDS ドキュメントセットを登録する機能を有すること。
② 登録メッセージは、ebRIM3.0 および ebRS3.0 メッセージ・フレームワークを使用し、MTOM や MTOM/XOP 形式の SOAP（Simple Object Access Protocol）メッセージであること。
③ ドキュメントセットは、ドキュメント及びメタデータを含み、ドキュメント、フォルダ、およびフォルダへのドキュメントの割り当てを正確に登録する機能を有すること。
④ ドキュメントセットのファイルタイプは、少なくとも PDF に対応し、ドキュメントソースからエクスポートされた PDF ファイルを簡便に登録可能とするアプリケーションユーザインタフェースを有すること。
⑤ PIX プロファイルにより、患者統合サーバに患者 ID 番号を検索できる機能を有すること。

3.4 PIX/PDQ 関連機能とその要件

この節では、PIX/PDQ に関する機能要件を示す。なお、実際の地域連携システム等に適用する場合は、それぞれの目的によって要求仕様は異なる。また、IHE の最新仕様などを確認して決定する必要があり、ここでは、要求定義の例を示す。

PIX （Patient Identifier Cross-referencing for MPI ）/PDQ（Patient Demographics Query）は、患者の識別のための仕組みで、各施設で管理されている患者 ID と同時に地域で一意な ID を発行管理する仕組みである。

PIX/PDQ は、地域内の患者を一意に識別する地域患者 ID を管理することを目

的として、患者基本情報のデータベースへの登録、更新、無効化を行い、患者基本情報問い合わせへの応答を行う機能を提供する。

図 3-5 は、施設間の患者 ID プロファイル PIX/PDQ に直接関与している各 IHE アクタのトランザクションを図示している。

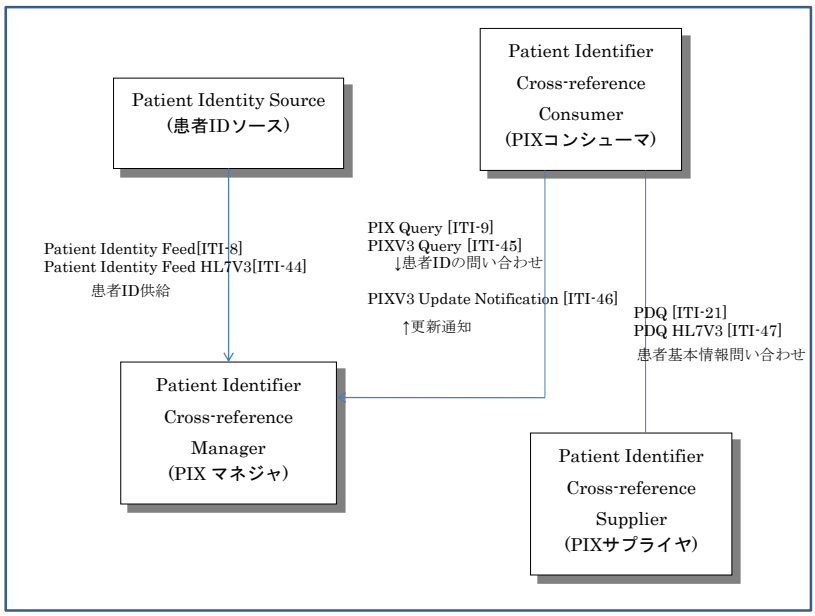


図 3-6 PIX/PDQ の IHE アクタおよびトランザクション関連

3.4.1 PIX 機能

PIX 機能に求められる要件は、以下のとおりである。

① PIX の PIX Manager (Patient Identifier Cross-reference Manager) は、Patient Identity Feed[ITI-8,ITI-44]、PIX Query[ITI-9,ITI-45] の２つのトランザクションをサポートすること。

② PIX は、患者情報管理システムは、地域内で患者を一意に識別する地域患者 ID を管理できること。

③ 患者基本情報は、HL7 メッセージ仕様で示される必須項目をセットできること。

④ 患者基本情報の登録要求時に、同一患者候補が PIX Manager に登録されていない場合には、PIX Manager は地域患者 ID を自動発番する機能を有すること。

⑤ 同一患者候補が PIX Manager に登録されている場合は、人間による判断により地域患者 ID を確定できる機能を有すること。

⑥ 患者基本情報項目の版管理の機能を有すること。

3.4.2 PDQ 機能

PDQ 機能に求められる要件は、以下のとおりである。

① PDQ は、Patient Demographics Supplier（アクタ）として、Patient Demographics Query[ITI-21,ITI-47]のトランザクションをサポートすること。

② PDQ は、地域患者 ID を発番するための患者基本情報の登録及び患者基本情報の問い合わせ（候補患者の問い合わせ）機能を提供すること。
③ 患者基本情報指定検索時には、同一患者の複数版のデータ(HL７メッセージにおける PID セグメントの繰り返し)の応答に対応する機能を有すること。
④ 患者基本情報検索時には、版管理データも検索対象とするものとする。

3.5 ATNA/CT 関連機能とその要件

この節では、ATNA/CT に関する機能の要件を示す。なお、実際の地域連携システム等に適用する場合は、それぞれの目的によって要求仕様は異なる。また、IHE の最新仕様などを確認して決定する必要があり、ここでは、要求定義の例を示す。

ATNA/CT の目的は、患者個人情報 PHI（Protected Healthcare Information）へのアクセスについて、「誰が」、「何を」、「どこから」、「どのサーバで」、「どのデータに対して」「どうしたか」を記録することである。

各セキュアなドメインは、ドメイン中にあるアクタの動作を、各トランザクションごとに監査証跡として記録する必要がある。

地域ドメイン内で、他の医療機関による監査証跡へのアクセスは、地域ドメインの業務に関する取り決めが、別途必要である。

通常の XDS 関連のトランザクションで生成されるべき監査証跡は、表 3-3 の通りである。

CT（Consistent Time)統合プロファイルは、ネットワーク上の多くのコンピュータのシステムクロックとタイムスタンプの正しい同期化を保証する方法を提供する。ATNA の監査証跡のデータ間の整合性を維持するには、CT による、複数のアクタとコンピュータ間の時刻を同期化する必要がある。

なお、ATNA/CT の機能の詳細は、附属書 C で解説する。

表 3-3 XDS に関連したトランザクションの監査証跡

対象トランザクション	説明
ドキュメントセット登録、及び ドキュメントセット提供登録：	・ソースは、ソースからレジストリへのPHIの取出しを表すExportイベントを生成する。トランザクション毎に監査証跡を作成する。 ・レジストは、ソースからレジストリへのPHIの取込みを意味するImportイベントを生成する。トランザクション毎に監査証跡を作成する。
ドキュメントクエリ：	レジストリは、クエリを記述したQueryイベントを生成し、クエリの結果がPHIを含む応答になった場合、Exportイベントを生成する。
ドキュメント取り出し：	リポジトリは、Exportイベントを生成する。これは、各ドキュメント取り出しトランザクションに１イベントであるか、または同じ患者には複数のトランザクションをまとめてもよい（この組合せの仕方はIHEでは定義されていない）。これは、監査証跡の量を軽減するためである。組合せが許されるのは、関与する利用者と患者が同一であり、時間の差が重要でないと考えられる場合である。

	ドキュメントコンシューマは、Importイベントを生成する。これはトランザクション毎に１イベントであるか、または複数のトランザクションをまとめて使用して、単一イベントとして報告してもよい。組合せが許されるのは、関与する利用者及び患者が同一である場合であり、時間の差が重要でないと考えられる場合である。
患者IDの登録：	患者IDソースは、Exportイベントを生成する。また、レジストリは、Importイベントを生成する。
画像ドキュメント取り出し：	画像ドキュメントコンシューマは、Importイベントを生成する。

3.5.1 ATNA 機能

ATNA 機能に求められる要件は、以下のとおりである。

① アクタ間の通信において、安全なノードのセキュア環境を提供すること。TLS（Trusted Layer Security）または同等の機能を用いるノードの通信としてセキュリティ要件を設計書に明記すること。

② 安全なノードと、監査情報を収集する監査リポジトリ(Audit Repository)ノード間で監査メッセージを通信する機能を有すること。

③ 監査対象ノード(各アクタ)に対する監査要件は、XAD(XDS Affinity Domain)固有情報は別途、詳細を決定するものとする。

④ 関連するプロセスの間のデータの整合性を維持するため、患者個人情報の不正な作成、参照、変更、削除などを容易に検出できる機能を有すること。

⑤ ノード間のネットワークアクセスを制限し、各ノードに対するアクセスを許可されたユーザだけに制限する機能を有すること。

⑥ セキュアドメイン内のセキュアノード間のネットワーク通信は、そのドメイン内の他のセキュアノードのみに制限する機能を有すること。

⑦ セキュアノードは、各 XAD において決定されるため、ローカル認証およびアクセス制御ポリシーを個別システムごとに指定し、許可されたユーザだけにアクセスを制限する XAD ユーザメンテナンス機能を有すること。

⑧ 不正操作の危険性を減少させ、部門監査を容易に実行可能とするため、XDS 関連アクタから監査レコードリポジトリへ監査レコード即時転送を行える集中的監査レコードリポジトリの機能を有すること。

⑨ IHE 対応トランザクションイベント以外にも、アプリケーションレベルのログイベント（データの検索ログ、エクスポートログなど）や、システムレベルのログイベント（OS エラーログ、ネットワーク通信ログなど）を収集し、管理可能な機能を有すること。

⑩ 患者個人情報の転送には、相互機器認証を行う機能 TLS もしくは同等の手段（例えば VPN）で全通信の暗号化を行う機能を有すること。

⑪ ATNA アクタの実装対象は、XDS 関連アクタである、ドキュメントレジストリ、ドキュメントリポジトリ、ドキュメントソース、画像ドキュメントソース、ドキュメントコンシューマ、画像ドキュメントコンシューマとする。それぞれのアクタ間通信を全て ATNA に準拠して動作させる仕様とすること。

3.5.2 CT 機能

CT 機能に求められる要件は、以下のとおりである。

① 複数のドメイン（インフラ）間で、セキュリティ及び情報収集のプロファイルを実行する際、複数のコンピュータにおける時刻の一貫性を保証する必要がある。それらの要求を満たす環境を構築し提供するものとする。

② CT プロファイルは、誤差中央値が 1 秒以下の同期化を指定するものとする。（これは、ほとんどの利用目的において十分な数値である）。

③ CT プロファイルは RFC 1305 で定義された Network Time Protocol (NPT)を利用して実現されるものとする。

④ タイムサーバがより上層のタイムサーバから時間を入手することを目的に、タイムクライアントとグループ化されている場合、タイムクライアントは NTP を利用するものとする。

⑤ タイムサーバとグループ化されていないタイムクライアントで、SNTP が利用可能な場合は、それを用いてもよい。

3.6 コネクタソン

3.6.1 コネクタソンとは

地域医療連携情報システムの構築にあたっては、多くのベンダの容易な参加を可能にするため、当然のことながら接続方式を標準化・統一する必要がある。これは前述のように IHE の統合プロファイルを適用することによって実現する方向で進められている。統合プロファイルの詳細仕様は、テクニカルフレームワークとして規定されており、このテクニカルフレームワークに基づいて各システムベンダは製品の開発を行い、相互接続性を検証する目的で製品を一堂に持ち寄り、規定された接続方式が守られているかの確認を実施している。この相互接続性の検証する場をコネクタソンと呼んでいる。

人によっては耳なれない“コネクタソン”なる用語は、Connect（システム間の接続）と Marathon（長時間をかけて行う）の合成語であり、もともとはインターネットの世界で、ネットワーク接続の規格について各社が実装したシステムの相互接続性を確認する場として使われたものであった。IHE 以前にも DICOM 規格に関連した接続性確認の場にコネクタソンの名称が使われていた。

3.6.2 IHE におけるコネクタソンの歴史

米国では IHE 発足まもない 1992 年から、毎年秋に約 1 週間かけて、放射線部門を中核としてコネクタソンが開催されてきた。その結果が 11 月末に行われる RSNA(北米放射線学会) でデモンストレーションされていた。その後、情報系の比重が上がった現在、春季開催の HIMSS (Healthcare Information Management System Society) におけるデモンストレーションにあわせ、年初に行われるようになってきている。

日本ではまず IHE の認知度を高めるために、毎年 4 月初頭に行われる JRC（日本ラジオロジー協会）の合同学会・展示会でマルチベンダ接続デモを先行させ、その接続確認の場をコネクタソンの準備としてもうけ、参加ベンダの習熟をは

かった。2003 年度に初めて国際的に認知される正式のコネクタソンの実施に至った。現在は、毎年 10 月に行われるようになり、海外からの参加ベンダも定着している。

日欧米とも放射線部門が先行した IHE コネクタソンも年々他部門への展開がはかられ、日本では 2006 年度から XDS の属する ITI（IT Infrastructure）の接続テストが実施された。参加ベンダ数、アクタ数とも増加しつつある。その実数などは、下記 3.6.5 項に記載されている日本 IHE 協会のホームページで確認することができる。

3.6.3　コネクタソンの実際

コネクタソンでは、統合プロファイルとアクタごとにテストシナリオが策定されており、参加ベンダはこのシナリオに従ってテストデータを用意し、テストを行う。接続すべきアクタを有する他社のシステムとの接続を行い（原則として 3 社以上)、所定のメッセージのやりとりが行われていることを検証する。各分野においての技術的専門的知識を有する審査員は、単にトランザクションやプロトコルが正常かどうかを判断するだけでなく、メッセージの中身についても確認を行っている。

3.6.4　接続性の担保について

従来から使われていた WEB ベースの進捗管理ツールに新たに日本で開発された接続検証ツールを組み込み、殆どの通信メッセージを保存するとともに文法チェックなどを自動的に行えるようになった。通信内容が自動的に解析され、審査員席のモニタ画面上にリアルタイムで表示されるため、検査精度の向上が図られるとともに審査の効率化も確認された。この日本発の接続検証ツールは、欧米からも注目されており、国際的に評価される時期が遠からず来るであろう。

将来は、ベンダの担当者や審査員が職場などにいながら、インターネット経由でコネクタソンが行える環境作りを各国がめざしており、このツールはその基盤となりうるものである。

3.6.5　コネクタソンのいわゆる“星取表”とその見方について

接続検証の結果は、結果表にまとめられ、俗称“星取表”として毎年公表されている。この結果表を用いて、医療機関はベンダがどの統合プロファイル、アクタをサポートしているかを確認することができる。

表は横軸に統合プロファイルとそれに必要なアクタを、縦軸はベンダ名となっている。このマトリックスの交点に記される「●」は、各統合プロファイルに定められた接続テストを実施し、所定の基準に合格したことを意味している。

これは、参加ベンダのシステムで実装されているアクタごとに、どの統合プロファイルにおいて所定の相互接続性を確保していたかを示すものである。原則として必須のテストシナリオについて他社の 3 システム以上と相互接続性が確認できたものを“合格”としている。

最新の星取表が、「IHE-Japan 2009 コネクタソン 結果表」である。過去の星

取表は日本 IHE 協会のホームページに掲載されており、以下の URL；
http://www.ihe-j.org/connectathon/index.html
で各年の評価結果一覧としてまとめられている。新しい年度では、コネクタソン状況・実施風景などの関連情報も見ることができる。

3.6.6 ユーザへの期待

以上述べたように、コネクタソンにおいては、順調に参加ベンダ・システム数も増加し、その結果としての星取表にのるアクタも漸増している。このように相互接続性は確保されつつあるが、医療機関においても、コネクタソンの結果をシステム導入時の採用基準に取り入れていただくとともに、地域医療連携情報システムの構築にあたって実際に使用する方々に必要な意味的相互運用性（semantic interoperability）の充実を図るべく関係者で協力してすすめれば、コネクタソンは質・量ともレベルアップアップするであろう。その成果は必ずユーザに還元されるはずである。

4.　ネットワーク基盤

本章では、地域医療連携情報システムのネットワーク基盤について考慮すべき事項を述べる。特に、「医療情報システムの安全管理に関するガイドライン」への対応、IHE におけるセキュリティ対策などについて解説する。なお、IHE ポリシーの Template などの関連情報を附属書 F に記載する。

4.1　ガイドラインへの対応

4.1.1　関連ガイドライン

(1)「医療情報システムの安全管理に関するガイドライン」(厚生労働省発行)

地域医療連携情報システムの構築に当たっては、その運用上の利便性と並行して、情報管理上の安全性を計る必要がある。この医療情報システムの安全管理に関して、行政より各事業者向けに参照すべきガイドラインが発行されている。中でも一番の基本となる「医療情報システムの安全管理に関するガイドライン」(厚生労働省発行　以下､「安全管理ガイドライン」と略す)が存在し 2010.3 には第 4.1 版に至っている。安全管理ガイドラインの経緯と法的位置づけの概略を図 4-1 に示す。

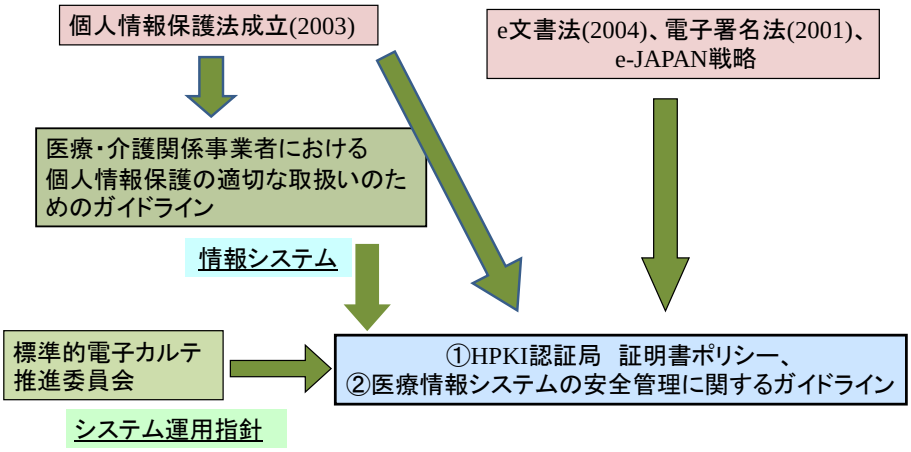


図 4-1　医療情報システムの安全管理に関するガイドラインの位置づけ

この中では医療機関向けに、医療機関内のみならず医療機関間における医療情報システム全般にわたり記載されている。情報システムだけでなく機能提供ベンダとの契約や、関係組織の責任分界の考え方や非常時の対応ガイドが記されており、地域医療連携情報システムに深く関係している。

図 4-1 からも分かる通り、個人情報保護法及び e-文書法が医療分野において執行される際の指針となるもので、医療情報を取り扱う際の法令の執行基準になるものである。本ガイドライン自体に罰則は無いが、ガイドラインに違背した状態は個人情報保護法及び e-文書法に求められる要件を満たさないと見做され、医療に関する多くの法令に違反したとされる可能性がある。

医療機関を対象にした安全管理ガイドラインを受けて、さらに、下図 4-2 の様に経済産業省、総務省発行のガイドラインが存在する。

(2)「医療情報を受託管理する情報処理事業者向けガイドライン」(経済産業省発行)

上記(1)が、外部に医療情報の保存を委託する医療機関向けのガイドに対応して、医療機関から患者情報を含む健康情報の受託管理を請け負う民間事業者向けに、準拠しなければならない内容が盛られている。

(3)「ASP・SaaS における情報セキュリティ対策ガイドライン」、「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」(総務省発行)

医療機関で用いる情報システムが ASP・SaaS という形で提供される場合、あるいは上記(2)が ASP・SaaS という形で提供される場合には、この 2 つのガイドラインへの準拠が求められる。「医療情報」への高度な安全管理の必要性が強調され、医療情報を取り扱うための専用ガイドラインが発行されている。

(4)「SaaS 向け SLA ガイドライン」(経済産業省発行)

一般的な SaaS サービス内容について両者で合意すべき項目が挙げられている。

上記(3)内においても「ASP・SaaS 事業者と医療機関との合意」が随所に要請されているが、このガイドラインによる「サービス利用のための合意」が参考になる。

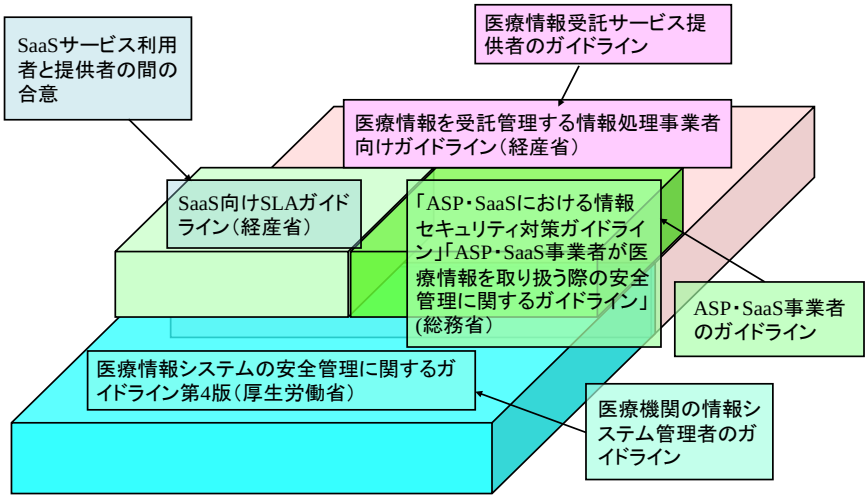


図 4-2 各ガイドラインの位置関係(厚生労働省資料から)

これらの行政発行のガイドラインに基づいて、学会や工業会などから個別システムについての具体的な場合についてのガイドラインが作られている。

本項の以下においては、主として安全管理ガイドラインをベースに記載を行う。

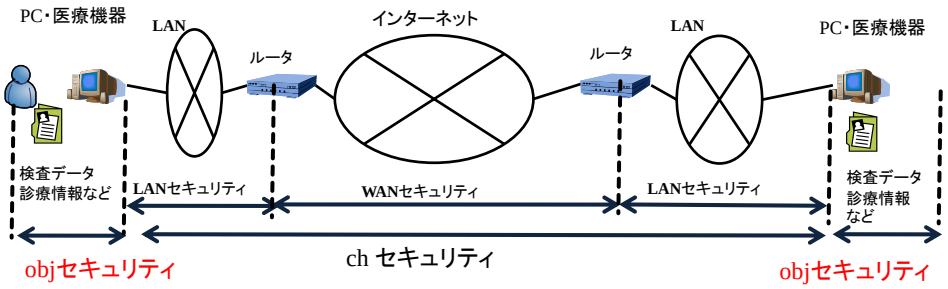
4.1.2　ネットワーク上の安全性

本節での「ネットワーク」とは医療機関内のネットワークではなく、医療機関外のネットワークについてである。医療機関外のネットワークに医療情報を流す場合には、個別の医療機関が運用管理責任を持てない経路を通過することになる。その経路設定の仕方、関係機関の責任分界の定め方について、安全管理ガイドラインで示されている。

安全管理ガイドラインの中で、医療機関が外部施設とネットワークを用いて医療情報を交信する場合の安全上の要求事項が示されている。技術的な詳細については、保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム(以下　HEASNET と略す)発行の「ガイドラインの実装事例に関する報告書」が参照先として示されている。

ここでは、オープンなネットワークで接続される場合を解説する。閉域 IP 通信網であっても、中間で閉域ネットワークが相互接続する場合は「オープンなネットワーク」とする。

安全管理ガイドラインにおいては、ネットワーク上での盗聴、改ざん、成りすましへの対応を、チャネル(ch)セキュリティ(回線上での暗号化などのセキュリティ)とオブジェクト(obj)セキュリティ(電子署名等の情報の内容へのセキュリティ)で要求している。以下の図 4-3 でこの概念を示す。



参照:HEASNET「ガイドラインの実装事例に関する報告書」

図 4-3　オープンなネットワーク接続のセキュリティ対策

(1) 技術的対策

セキュリティ対策の目的は、意図した宛先にのみ、安全に送信されることである。オープンなネットワーク上には図 4-4 に示す脅威がありチャネルセキュリティ対策が必要である。安全管理ガイドラインではネットワーク種別の選定基準・安全管理(6.11 章)とネットワーク事業者との責任分界の考え方(4 章)を示している。

①チャネルセキュリティの確保

通信の起点・終点識別の認証と成りすましへの対策(相互認証)として、IPSec+IKE で実行すること。

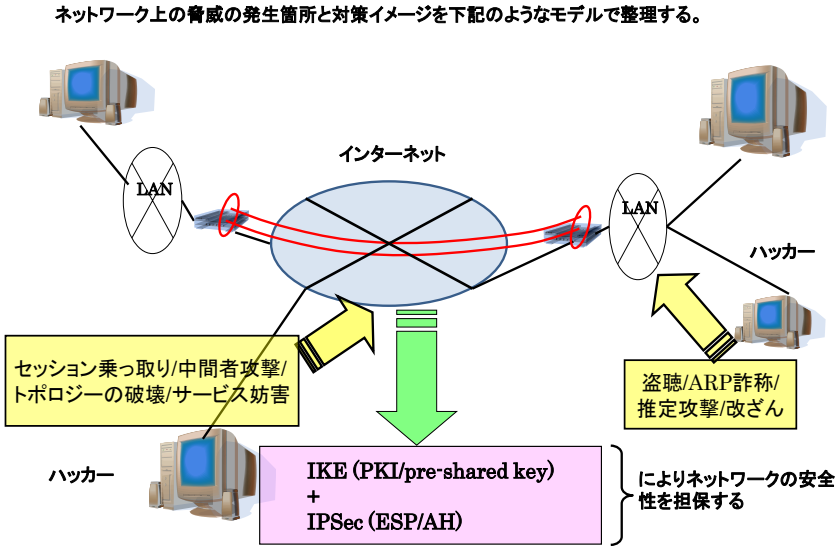


図 4-4 オープンなネットワーク上の脅威とチャネルセキュリティ対策

(HEASNET 資料から)

参考資料である HEASNET の資料では、VPN 利用でも設定によっては危険があり、以下の 4 つの対策を求めている。

◆ **VPN 接続経路の分離**

通信ルートを分けることで外部からの不正なアクセスを防止し、VPN 接続のセキュアな経路を確保する。インターネット接続点において、VPN 接続とそれ以外の一般的な接続とで経路を物理的に分離し、VPN 接続の場合は FW 透過後に必ず認証によって適正な接続が担保されるようにする。

◆ **異なる VPN 間の経路制御**

リモート保守や情報提供サービスにおいて、契約に定められたリソース以外への不正なアクセスを防ぐため、ローカル拠点のホストまたは IP アドレスレベルで制御し、拠点間で接続された VPN によって拠点内の許可されていないリソースに対してアクセスされないような制限を設ける。

◆ **VPN 間の不正中継禁止**

ある拠点(A)と他二者(B、C)間の契約(A-B、A-C 間)で形成された 2 つの VPN 接続によって、これらの契約の当事者でない 2 つの拠点(B、C)間での VPN 接続(B-C 間)ができないよう、ある拠点を経由しての不正な中継アクセスを禁止する。

◆ **ゾーンの分離**

VPN 接続をする端末が配置された VPN 専用ゾーンとそれ以外の通常接続用ゾーンを設け、不適切なホストからの VPN 接続を防止する。VPN 接続専用ゾー

ンと通常接続用ゾーンの間の通信を制限する。

②オブジェクトセキュリティの確保
盗聴への対策として暗号化(電子政府推奨暗号を使用)、改ざんへの対策として電子署名(HPKI)＋タイムスタンプを施すこと。
電子署名環境の用途には、HPKI(Health Public Key Infrastructure　健康公開鍵基盤)で医療資格者の署名用電子証明書発行の仕組みを定めている(図 4-1)。

③相互認証
日本で一意に特定できる厚生労働省認定の要のある通信相手の資格確認には、HPKI で医療資格者と保健医療機関の認証用電子証明書発行の仕組みを定めている(図 4-1)。

(2) 運用的対策
関係者間の契約を含めての運用的対策では、責任分界点を明確化して、管理責任の空白を作らないことである。

①情報の送信側・受信側の責任分界点
送信側はどの時点までが責任範囲か、受信側はどの時点から責任が発生するかの明確化

②通信を形成する事業者の責任分界点
ネットワークを経由する情報伝送では、送信側・受信側のどちらでもない事業者の管理運営する経路を通過するのが普通である。上記①の情報の送信側・受信側だけでなく、回線事業者、ネットワークサービス提供者を含めた関係事業者間で、誰がどこまで何を担保するか、ネットワークサービス提供者の管理責任範囲はどこまでか、の管理責任範囲を明確化し、事故発生時の一義的対応者を定めておくことが求められている。

4.2　IHE におけるセキュリティ対策

(1) IHE と安全管理ガイドラインの記載範疇
IHE は相互接続性のための技術仕様を中心に述べているものであり、IHE-ITI(IT Infrastructure) では、XDS として地域連携における情報共有の基盤の仕組みを述べている。また、XDR として 1:1 の医療情報送受信の仕組みを述べている。
技術仕様としては、セキュリティ機能(DSG)、通信技術(SOAP)、ネットワーク環境(TLS)　などを挙げている。
更に、運用全般のガイドとして「ITI　User Handbooks」として、(2)以降に述べる 3 文書を発行してセキュリティ対策のガイドを示している。
当然であるが、IHE に従って実装する際の具体的内容は各医療機関で決める必要があり、IHE の機能だけでは 4.1.1 のガイドラインには適合が出来ない。
安全管理ガイドラインでは、概略以下のような対応を求めている。

- 盗聴・改ざん・成りすまし対策をすること。
- 契約も含めて、責任の空白地帯を作らないこと。
- オブジェクトセキュリティ、チャネルセキュリティ、相互認証をすること。
- 署名の必要な文書への電子署名・タイムスタンプを施すこと。
- 診療記録の保存を受託する民間事業者には経済産業省、総務省のガイドラインに適合すること。
- 具体的なネットワーク環境毎のセキュリティ対策を記載している。

双方の記載範疇の差の概略は図 4-5 の通りである。

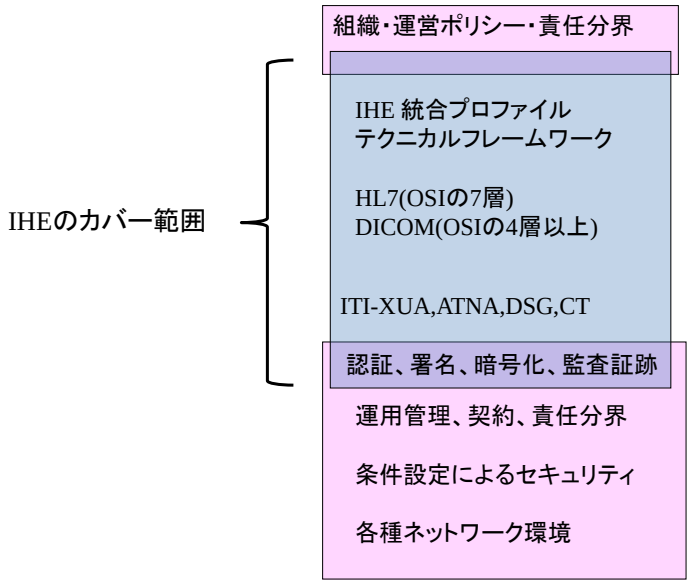


図 4-5 IHE と安全管理ガイドラインの記載

(2) HIE Security and Privacy through IHE Profiles

本文書においては、複数医療機関が一人の患者の診療情報を長期に共有する仕組みである HIE (healthcare Information Exchange)において、Security と Privacy に的を絞ったポリシー策定事項を述べている。IHE のプロファイルは相互運用性の確保に必要な技術的詳細の取決めであり、

Privacy and Security Polices、Risk Management、Operating Systems、Healthcare Application Functionality、Physical Controls、 General Network Controls

については触れていない。患者のプライバシと情報セキュリティを守るため技術だけでなく、ポリシー定義が重要であり、本文書はプライバシとセキュリティのために、IHE プロファイルの使い方を示している。

既に定められている統合プロファイルのなかで、Security と Privacy に関する統合プロファイルは下記がある。

- Audit Trail and Node Authentication (ATNA)
- Consistent Time (CT)
- Basic Patient Privacy Consents (BPPC)
- Enterprise User Authentication (EUA)
- Cross-Enterprise User Assertion (XUA)
- Personnel White Pages (PWP)
- Digital Signatures (DSG)
- Notification of Document Availability (NAV)

XDS あるいは XDR、XCA モデルでシステムを構築する場合は、これらの機能を用いて安全管理ガイドラインの要求事項を満たすことが有用である。附属書 F を参照。

(3) Cookbook: Preparing the IHE Profile Security Section

本文書は、一般的なセキュリティ対策の準備手順を紹介している。附属書 F を参照。

(4) Template for XDS Affinity Domain Deployment Planning (以下 Template と略す)」

本文書に、地域医療連携情報システム構築のためのポリシー作成ガイドを示している。(1)で示すポリシーは Security と Privacy に的を絞ったものであるが、本文書は、ある地域における単独 XAD、複数の XAD 間連携(XCA)のポリシーを定義する場合の「決めるべき事項」の雛形として使用できる。

個人情報保護方針、文書形式と内容、役割とアクセス権限の有る文書定義、運営組織等のポリシーに関わる内容等、があり、XDS モデルを採用しなくても役立つ文書である。セキュリティについても多くのページを割いて示してあり、安全管理ガイドラインとの関連も深い。4.3 で項目の紹介をする。詳しくは附属書 F を参照。

4.3 個別システムで指定すべき事項

近年の課題である地域における医療施設連携による医療サービス提供のシステム形態については、IHE により XDS モデルが作成され日本のいくつかの地域でも、このモデルを参考にした地域医療連携システムが構築されている。また、IHE XDS モデルを意識せずに幾つかの地域連携システムが運用されている。

また、特定の機関間で医療情報を 1:1 で交換する XDR モデルの形も広く用いられている。

モデルを XDS 型と XDR 型の 2 タイプで考慮すべき事項の考察をする。

(1) 共通事項

どのモデルであっても、安全管理ガイドラインが要求する事項は満たす必要がある。

特に、①運用管理規程の作成・運用、②責任分界を定めた契約の締結、③ベンダの標準化に対する方針の確認、④ネットワークサービス事業者の選定における条件(例えば、HEASNET の報告書内容が判るベンダ、HISPRO の評価を得てい

るベンダ)、は必須である。

4.2(4)に紹介した IHE の Template 内容は、XDS を構築する際の参加機関での合意事項を作成する際の参考になる。以下に項目概要を列挙する。詳しくは附属書 F を参照。

上記①には A5 を、②には A8 を、参加事業者の意思統一には A4 と A6 を参考にすると便利である。

表 4-1 IHE Template の記載項目

A.1 はじめに
A.2 Glossary
A.3 参考資料
A.4 組織的規約
A.4.1 組織構成
A.4.2 組織的規約
A.4.3 資金提供
A.4.4 透明性
A.4.5 施行と是正
A.4.6 法的問題（法的統治性、義務とリスク配分、免責、発行物への知的財産権）
A.5 運用規則
A.5.1 サービスレベルの合意
A.5.2 日常的運営
A.5.3 システム停止の管理
A.5.4 構成管理
A.5.5 新機能要素の追加
A.5.6 データ維持、保存、バックアップ
A.5.7 不具合の回復
A.6 メンバの規約
A.6.1 入会
A.6.2 メンバのタイプ
A.6.3 メンバ方針
A.7 XAD の外部からの接続性
A.7.1 相互運用性規約
A.8 システム構造
Business Actors、Technical Actor 仕様（レジストリ、リポジトリ、ドキュメントソース、など）
A.9 用語と意味
A.10 患者プライバシと同意
A.10.1 ドキュメントのアクセスと利用の一般則
A.10.2 患者同意（BPPC）
A.10.3 プライバシを越える時のガイド
A.11 技術的セキュリティ

(2) IHE XDS モデルでの形態

図 4-6 に XDS での医療連携シナリオを示す。
この図についての説明は IHE に関する多くの箇所で行われているため、本書ではシナリオ自体については省略する。安全管理ガイドラインとの間では、XAD(XDS Affinity Domain:XDS のポリシーに同意した参加者によるコミュニティ)、レジストリ(各診療データの存在箇所を示す管理台帳)、リポジトリ(XAD 参加の各医療機関が他医療機関に開示する診療情報保管庫)の 3 つが関与する。

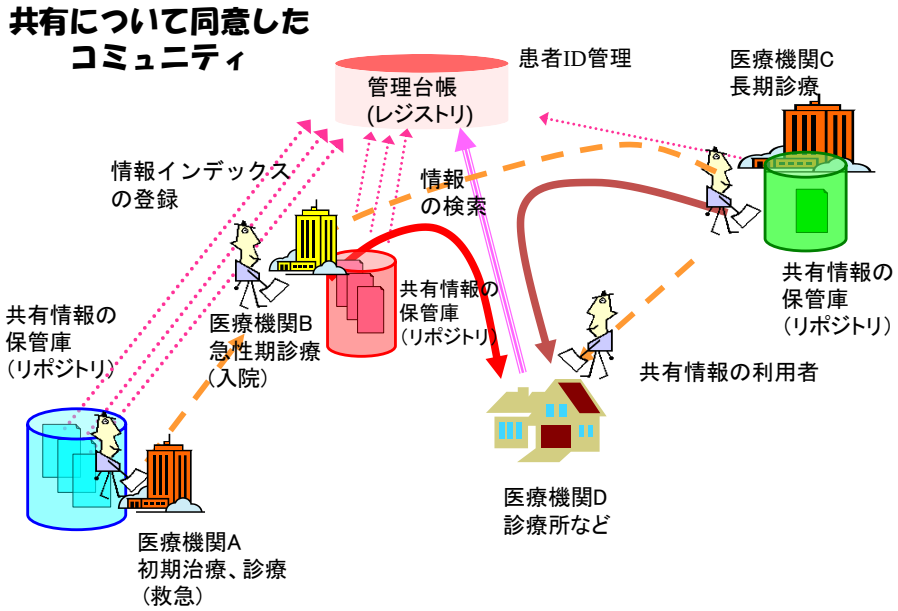


図 4-6 XDS での医療連携シナリオ

①データの取り扱いの考え方
a. 委託、第三者提供、共同利用
医療機関から外部に診療データを提供する場合は、委託か第三者提供かの厳密な定義があり、責任の在り方が違ってくる。
委託とは、委託契約に基づき業務の一部(例えば臨床検査)を外部機関に託すもので、その情報の管理責任は一義的には委託元にある。委託元は委託先の情報管理を監督しなければならない。
第三者提供とは、患者等の同意で他事業者に渡す(例えば紹介状による治療情報提供)こと、あるいは法的な要求で提供することで、第三者に確実に情報提供が行われた時点で情報の管理責任は提供先に移動する。
また、診療目的での共同利用ならば第三者提供に当たらないので、本人同意は不要とされているが、その条件は下記のように定められている。
「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン　Ⅲ５第三者提供（４）第三者に非該当ケース、共同での利用に必要な条件」において、
「(ア) 利用する個人データ項目、(イ) 利用者の範囲（個別列挙か明確な特

定)、 （ウ）利用目的、(エ）個人データの管理責任者の氏名又は名称 」が書かれてあり、診療情報を「共同利用」するためには、個人データを特定のものとの間で共同して利用することを明らかにし、利用する個人データ項目、利用者の範囲、利用目的、個人データの管理責任の所在等をあらかじめ本人に通知等をしている必要がある。

したがって、IHE XDS モデルと言うだけでは、上記の要件を満たしていない可能性があり、他の施設での診療情報の利用は第三者提供にあたる可能性がある。参加医療機関でのデータ授受の性格(委託か第三者提供か)とタイミングの合意を計っておくことが必要である。

b. レジストリへの提供

レジストリ運営組織には各医療機関から「データ提供業務の委託」になるようにし、委託契約と管理責任や監督義務を果たすことが、XDS を実装する上では安全管理ガイドラインに適合しやすくなると思われる。

c. レジストリでのデータ保管

レジストリはデータが存在するリポジトリのインデックスであり医療情報そのものではないが、機微なプライバシに関与する医療情報の存否を示し、且つ長期の保管が前提であるため、医療情報の外部保管と同等に扱うことが求められる。そこで、レジストリを民間などのデータセンターを利用する際には、経済産業省発行の「医療情報の委託を受ける民間事業者向けガイドライン」 を参照して、外部保存に準拠した管理運営をする必要がある。

d. 外部保存の基準

外部保存として扱い際には、安全管理ガイドライン「8.1.2　外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準 」の「B. 考え方　 2. 情報の取り扱い」に従う必要がある。そこでの記載には「病院、診療所、医療法人等が適切に管理する場所に保存する場合病院、診療所等であっても、保存を受託した診療録等について分析等を行おうとする場合は、委託した病院、診療所及び患者の同意を得た上で、不当な営利、利益を目的としない場合に限る。

また、実施にあたっては院内に検証のための組織等を作り客観的な評価を行う必要がある。匿名化された情報を取り扱う場合においても、地域や委託した医療機関等の規模に よっては容易に個人が特定される可能性もあることから、匿名化の妥当性の検証を 検証組織で検討したり、取り扱いをしている事実を患者等に掲示等を使って知らせたりする等、 個人情報の保護に配慮する必要がある。」とある。

(3) IHE XDR モデルでの形態

複数医療機関で医療情報を共有するのではなく、特定の医療機関同士で診療データを交換するモデルである。典型的な例が下図 4-7 の「遠隔画像診断支援サービス」である。

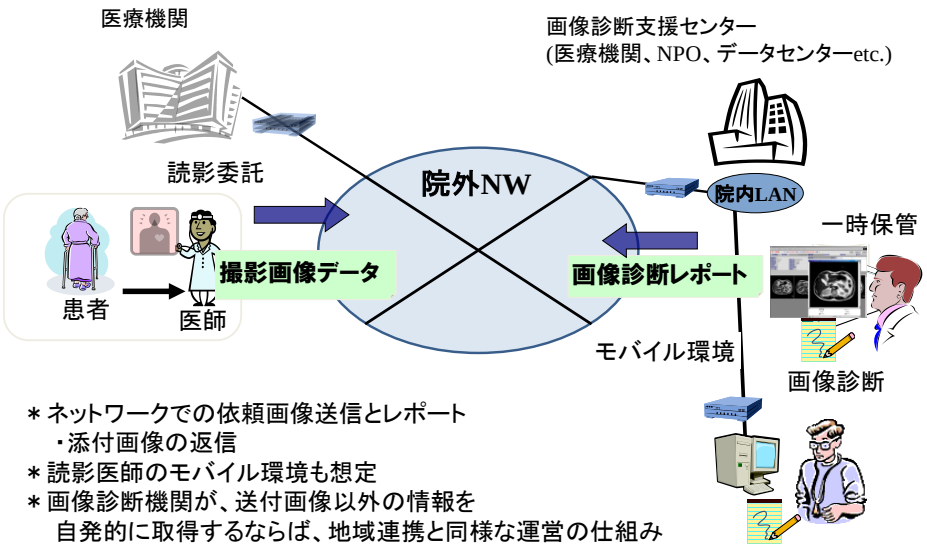


図 4-7 XDR での医療連携シナリオ

この例では、画像診断業務を契約により他医療機関に委託することであり、その中での医療情報の取扱い方については、安全管理ガイドラインの 4.3 に「医療機関等の業務の一部を委託することに伴い情報が「一時的に外部に保存」される場合ここでいう委託とは遠隔画像診断、臨床検査等、診療等を目的とした業務の第三者委託であり、これに伴い一時的にせよ情報を第三者が保管することとなる。

医療機関の管理者は業務委託先に対して、受託する事業者の選定に関する責任や（セキュリティ等の）改善指示を含めた管理責任があるとともに、情報の保存期間の規定等の管理監督を行う必要がある。

ただし、受託する事業者は保存した情報の漏えい防止、改ざん防止等の対策を講じることは当然であるが、感染症情報や遺伝子情報等機微な情報の取り扱い方法や保存期間等を双方協議し明記しておく必要がある。」の記載がある。

画像診断を受託した施設で医療情報の長期保存をするならば「外部保存」の条件を意識する必要がある。

上記(2)、(3)のモデルを簡単に比較すると下表のようになる。両タイプの違いを認識して対処を行うことが求められる。

表 4-2 XDS と XDR モデルの比較

	遠隔画像診断	地域連携
ネットワーク上の安全措置と契約	運用管理規程、NW上の安全措置、責任分解の明確化と契約	
標準化	ベンダ選定条件、コード、プロトコル、セキュリティ	
患者の行動	特定の1医療機関に訪れる	複数医療機関に訪れる
データ取り扱いの考え方	読影業務の委託 ⇒ 管理責任、監督義務 画像表示の同一性	共同で診療にあたる場合⇒同意不要 第3者提供になる場合⇒同意が必要 レジストリには委託
データアクセス	医療施設から読影医療機関に直接送付、レポートの直接返信	レジストリ経由でレポジトリへアクセス
モデル	XDR、XDS-I ・部門システム内にNW ・部門システム外で施設間連携	XDS、XDS-I

4.4 ネットワークのガイドライン適合性評価（HISPRO）

各医療機関において、安全管理ガイドラインに適合するオープンなネットワーク機器・サービスを選定することは、通信の専門家の少ない医療機関では面倒なことである。そのため、「実効性」を確保しつつユーザ視点で「安全性を客観的に評価する」ことを目的に、利用者である、日本医師会、日本薬剤師会、また、医療 IT の専門集団である日本医療情報学会を設立時社員とする法人「一般社団法人保健医療福祉情報安全管理適合性評価協会（Health Information Security Performance Rating Organization ： HISPRO)」が設立されている。

最初の評価対象として、レセプトオンライン請求の IPsec+IKE を用いた回線について、医療情報システムの安全管理に関するガイドラインに沿った評価を実施し、評価製品を公表している。

ネットワーク機器・サービスの選定に当たっては、参考にすると便利である。

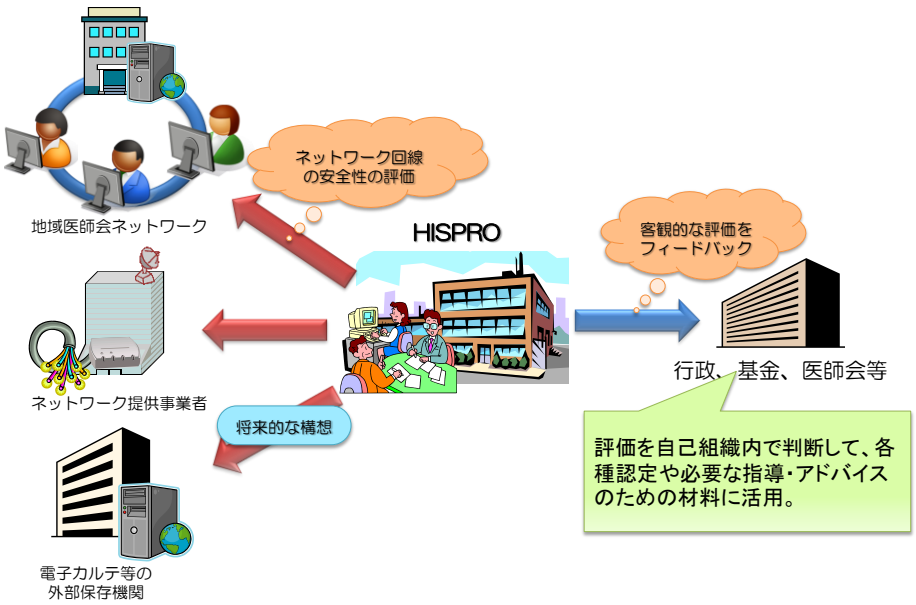


図 4-8 HISPRO の役割

評価を実施する際の主観点は、以下の内容である。

- 接続中継地点がある場合電気通信事業法に従い、事業の届出を行っている事業者であること
- 評価対象となるサービスの契約書およびサービス仕様書が提示されていること。
- サービスの提供範囲、責任範囲が明確になっていること
- 顧客情報を適切に管理することが明文化されていること
- サービス拠点の物理セキュリティや災害に対する対応が明確になっていること
- サービス設備のセキュリティが確保されていること
- サービス設備のシステム障害などを考慮した BCP(business continuity plan)が確立していること
- システム監視や障害発生時の連絡方法、故障復旧体制について記述されていること
- 合意された内容に沿った通信設定がされていること（通信の合意をしていない拠点との通信やアクセスができないようになっていること）が明確になっていること
- 暗号化通信において適正な技術を適用していること
- サービスに使用する医療機関の終端装置の製品情報および仕様が明確になっていること
- 医療機関のセキュリティを守るために終端装置の設置個所から院外までのセキュリティ対策実施を喚起していること

5. システムの運用に関すること

本章では、地域医療連携情報システムの運用に関する事項について、体制、契約、保守管理などについて説明する。なお、システム発注時に考慮すべき提案依頼事項については、附属書 G に述べる。

5.1 システム運用に必要な体制と契約

地域医療連携では参加施設間の意思疎通が重要であり、情報システムの運用管理においても同様である。情報システムの仕様は地域連携システムの運営組織に依存するため、医療機関とシステムベンダが密接に協力して、システム構築できる体制が必要である。医療情報システムの安全管理に関するガイドラインには、外部機関と診療情報等を連携する場合に取り決めるべき内容について定義されている（表 5-1)。[1] 地域医療連携システムを構築して外部の機関と診療情報共有の連携等を行う場合には、連携医療機関同士、医療機関とシステムベンダ、医療機関と通信事業者の間で取り決めが必要となる。本節では、運用的な観点からシステム構築に必要な体制と契約について説明する。

表 5-1 外部機関と診療情報等を連携する場合に取り決めるべき内容

（医療情報システムの安全管理に関するガイドラインより）

項目	内容
組織的規約	理念、目的 管理と運営者の一覧、各役割と責任 医療機関と情報処理事業者・通信事業者等との責任分界点 免責事項、知的財産権に関する規程 メンバの規約（メンバ資格タイプ、メンバの状況を管理する規約)、資金問題 等
運用規則	管理組織構成、日常的運営レベルでの管理方法 システム停止の管理（予定されたダウンタイムの通知方法、予定外のシステムダウンの原因と解決の通知等)、データ維持、保存、バックアップ 、不具合の回復 等
プライバシ管理	患者共通 ID（もし、あるならば）の管理方法 文書のアクセスと利用の一般則 役割とアクセス権限のある文書種別の対応規約 患者同意のルール 非常時のガイド(ブレークグラス､システム停止時､等の条件） 等
システム構造	全体構造、システム機能を構成する要素、制約事項 連携組織外部との接続性(連携外部の組織とデータ交換方法） 等
技術的セキュリティ	リスク分析 認証、役割管理、 役割識別(パスワード規約、2 要素認証等の識別方法) 可搬媒体のセキュリティ要件 等
構成管理	ハードウェアやソフトウェアの機能更新、構成変更等の管理方法、新機能要素の追加承認方法 等

監査	マニュアルの整備、守秘契約、退職後の守秘規程、 規程遵守の監査 何時、誰が監査し、適切な行動が取られるか
規約の更新周期	

5.1.1　システム運用体制

地域医療連携を行う目的、参加する施設の数などによって多様なシステム運用形態が考えられるが、ここでは『地域医療連携システム運用協議会』を設立して、医療機関にレジストリ、リポジトリを設置して情報システムを管理することを仮定する。(図 5-1)[1]　協議会ではレジストリ管理、セキュリティ監視、ネットワークの管理、利用者の訓練、ユーザからの問い合わせや苦情相談を受け付ける。また、ユーザ登録や患者の名寄せ管理の業務を行うことも考えられる。

医療機関で個人情報を管理する場合、ガイドラインの 8.1.2 節 「外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準」のうち、「病院、診療所、医療法人等が適切に管理する場所に保存する場合」に従って、安全管理を行う必要がある。協議会には医療スタッフのほか、医療機関の情報システムの管理者、情報システムの開発保守業者などが参加して、継続的に運用を話し合う体制を構築する。

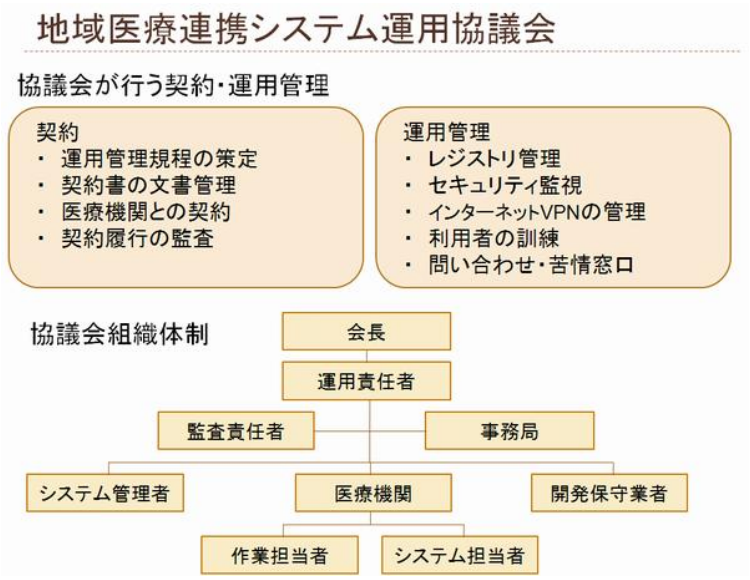


図 5-1　地域医療連携システム運用協議の組織図(例)

[1] ここでは、医療機関にデータを保存することを仮定したが、この他に行政機関等が開設したデータセンター等に保存する場合、医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合が考えられる。ガイドラインの 8 章を参考にして、それぞれに対応した情報の取り扱いに関する契約を結ぶ必要がある。

5.1.2　システム運用に必要な契約

医療機関は、連携する医療機関、開発保守業者、通信事業者と表 5-1 に示す項目などについて契約を取り交わす必要がある。連携医療機関が少ない場合などは、個別に契約を結んでも良いが、連携医療機関が増えると組み合わせの数だけ契約しなければならず、非効率的である。そのため、ここでは協議会を中心として、医療機関と協議会、開発保守業者と協議会、通信事業者と協議会で契約を結ぶことを仮定している。それぞれの契約において、責任分界点を明確にし、地域連携に必要な契約を締結する。運用管理規定の文例はガイドラインの付表１にあるので参考にされたい（[1]参照)。

表 5-2　地域医療連携システムの構築に必要な契約(例)

運用協議会（または、主体となる医療機関）と医療機関の契約
情報処理関連事業者と運用協議会の契約
通信事業者と運用協議会の契約

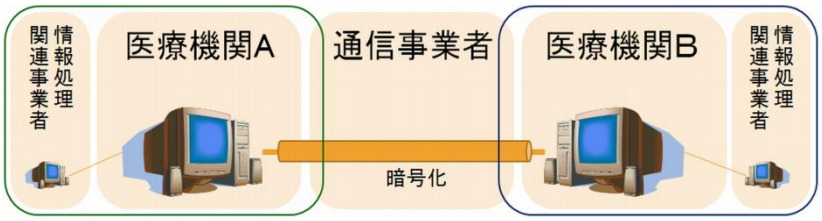


図 5-2 地域医療連携を行う際の医療機関、開発保守業者、通信事業者の関係

（１）運用協議会（あるいは、主たる医療機関）と医療機関の契約

医療機関と協議会の間の契約では、運用管理規程の遵守、責任分界点、個人情報の保護に関する契約を行う必要がある。責任分界点については通信経路、通常運用における責任、事後責任にわけて考える。個人情報保護に関する契約では、患者の同意に関する契約、ユーザ認証・識別・アクセス管理に関する契約を行う必要がある。個人情報保護の観点から、医療機関においては、患者に地域医療連携システムに用いることに対する、同意を取る必要がある。また、情報漏えいや不適切な閲覧が起こらないような装置についても規定する必要がある。連携医療機関同士の取り決め事項、契約事項については、4 章で紹介されている IHE-ITI のテンプレートを参考にされたい。

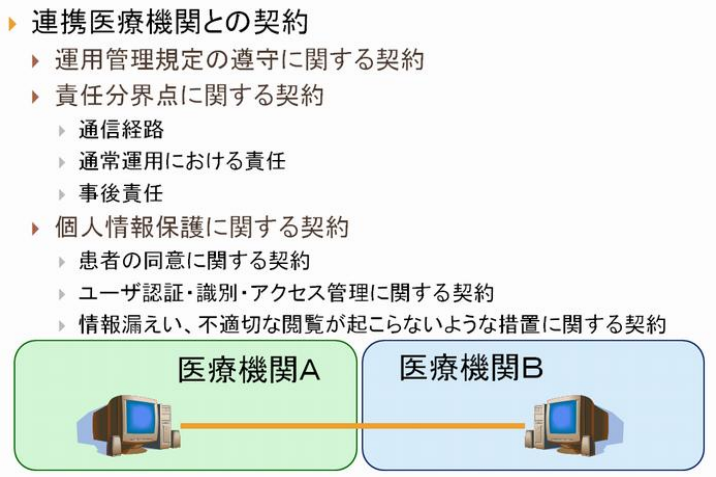


図 5-3 運用協議会と医療機関が結ぶべき契約

（２）運用協議会（あるいは主たる医療機関）と情報処理関連事業者との契約

医療機関と開発保守業者の間の契約では、協議会が定めた運用管理規定の遵守することを明記する必要がある。また、通信経路における責任分界点を示して、運用上における責任と事後責任について明記するべきである。守秘契約は、地域医療連携に参加する他の医療機関を包含する必要がある。

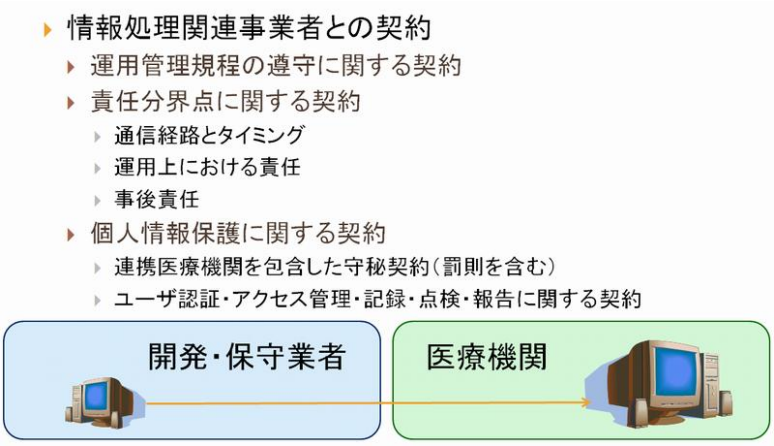


図 5-4 運用協議会と開発・保守業者が結ぶべき契約

（３）運用協議会（あるいは、主たる医療機関）と通信事業者との契約

通信事業者との契約では、通信経路の責任分界点を明らかにして管理責任、事後責任を明確にすることが必要である。地域医療連携システムを構築するためのネットワーク基盤については、４章を参照されたい。

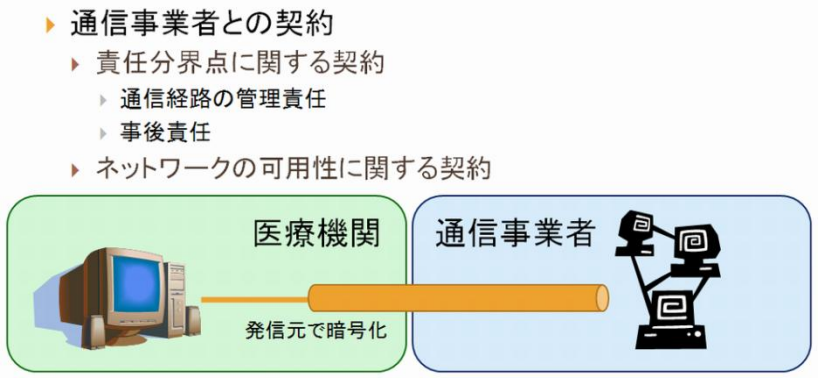


図 5-5 運用協議会と通信事業者が結ぶべき契約

5.2 情報システムの保守管理

医療情報システムの安全管理に関するガイドラインでは、組織的、物理的、技術的、人的な側面での安全対策など、様々な管理対策を求めている。地域医療連携システムを構築する際には特に、組織的安全対策、技術的安全対策、人的安全対策が重要であり、外部と個人情報を含む医療情報を交換する場合の安全管理についても対策を検討する必要がある。

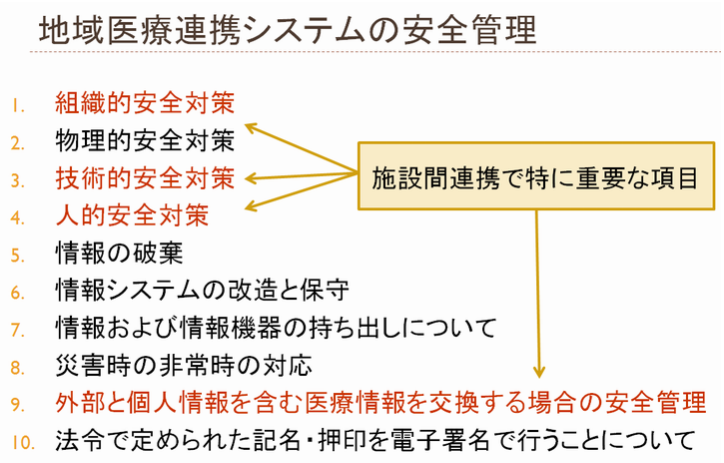


図 5-6 地域医療連携システムを構築する際に重点を置くべき安全管理項目

5.2.1 通常運用における安全管理対策

通常運用における安全管理では、図 5-7 に示す項目について規定する必要がある。このうち、組織的な面では作業担当者の限定や文書管理、事故対策、利用者への周知法などについて検討する必要がある。また、人的な面ではではアクセス権限の付与を複数の医療機関のなかで行う方法を取り決める必要がある。

技術面では、リモートメインテナンスの方法、アクセスログの収集や、無線 LAN に接続された端末の使用についてのルールを取り決める必要がある。

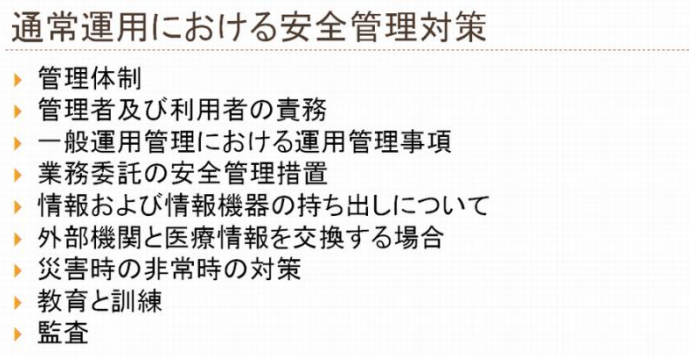


図 5-7 地域医療連携システムの通常運用に必要な安全管理項目

5.2.2 機器の保守管理

地域医療連携システムは医療情報を扱うので、たとえ診療情報の原本は別のサーバに保存されていたとしても、診療情報の真正性、見読性、保存性は確保して運用すべきである。機器の保守管理について、システム改修を行う場合などの責任範囲については、あらかじめ明確にしておくべきである。

5.2.3 患者への説明と同意

レジストリに記録される情報や、連携医療機関に提供される医療情報について、個人情報の保護に関する対策が必要である。患者には、外部保存に関する説明と同意が必要である。また、外部保存の契約終了時にどのように処理をするか、など取り決める必要がある。

5.2.4 教育訓練および監査

人的安全対策の観点から、利用者に対してはシステムの利用方法と、個人情報保護、医療情報セキュリティに関する教育を定期的に実施するべきである。また、組織的安全対策の観点から、安全管理対策の充実をはかるため、定期的な監査の実施が効果的である。

5.2.5 トラブル発生時の対応

トラブル発生時には、医療機関が主体となって対応が重要である。万一の場合に備えて、管理・責任体制を明確にしておく必要がある。また、データの授受に支障が生じた場合の対処方法、情報漏洩に対する対処方法、問合せ・苦情に対する対処方法をあらかじめ決めておくことが重要である。

引用文献

[1] 厚生労働省. 医療情報システムの安全管理に関するガイドライン 第 4.1 版. 2010.2.

6. まとめ －XDS の応用範囲の広がりへの期待

本ハンドブックは XDS を構築するための考え方から具体的な事柄を含めまとめられています。読者はこれを利用して XDS を現実のものとして実現し役立つシステムとして活用していただければ幸いです。本章では今後期待される XDS の応用分野の広がりを述べてまとめとします。

6.1 地域医療連携適用分野の広がり

XDS は経済産業省が平成 18 年度から「地域医療情報連携システムの標準化及び実証事業」の中で、東海ネット医療フォーラムが受託し、脳卒中医療を対象とする地域連携パスの情報共有システムに関して実証されました。

一方、平成 18 年度の医療制度改革で、都道府県は、４疾病（がん対策、脳卒中対策、急性心筋梗塞対策、糖尿病対策）及び５事業（救急医療、災害時医療、へき地医療、周産期医療、小児医療）のそれぞれについて医療計画に医療連携体制を明示することになっています。こうした場合、特に地域連携クリティカルパスによる情報共有が重要となってきます。

標準的な連携基盤の構築により脳卒中医療により実証された経験や手法がこうした分野へ広がってくることが期待されます。

6.2 地域見守りシステムへの広がり

XDS は前項で述べた医療関係者の連携ばかりでなく、「地域見守りシステム」すなわち介護を含めた広い範囲の地域の関係者が見守るためのシステムへも応用が可能です。この場合、情報の共有範囲や種類を個人や家族の同意の下に管理できるセキュリティの仕組みが重要になってきます。また、情報リテラシーに格差がある中での利用となるのでシステムの簡便さや即時性が課題となってきます。

現在、紙ベースで行なわれている見守りが、出来るだけ自動的に情報システムに入力され、情報が適切に共有されることにより、個人ごとに適した見守りが実現されることが期待されます。

6.3 電子私書箱構想による個人健康情報活用システムへの広がり

地域医療連携情報システムは医療関係者同士の情報共有が主たる目的であるので、患者がこうしたシステムを利用することに同意した場合は自動的に医療施設間で連携に必要な患者やデータが共有されることになります。

電子私書箱構想による個人健康情報活用システムは個人の視点で健康情報を保管管理するもので、そのデータの入力に電子私書箱構想を活用します。

電子私書箱は個人に対して予め定められたアカウントがあってこれに対して個人が希望するデータを送付してもらう仕組みです。住民登録された住所の自宅のポストのように住民票の登録先と同等な本人確認ができるアカウントですと、法律的に本人確認が必要な情報も送りつけることが出来ます。この為、最低限の基盤が公的に作られることが期待されます。電子私書箱構想はももとも

と、年金等の公的なデータを個人へ送付する、丁度、電子申請システムが官へのアップ機能とすればダウン機能を構築することに当たります。

個人が情報を受け取る部分やその情報を生涯保存する為のポータルサイトはXDS でいう、レジストリとリポジトリに分けると標準的なソフトウェアがつかえるので構築されやすくなります。また、トランズアクションも XDS と同様なものが使用できるので、XDS との共通化を進めておくと便利な点が多いと思われます。

その為には電子私書箱構想のユースケースを定め IHE 手法を用いて、プロフィルにまとめておく必要があります。

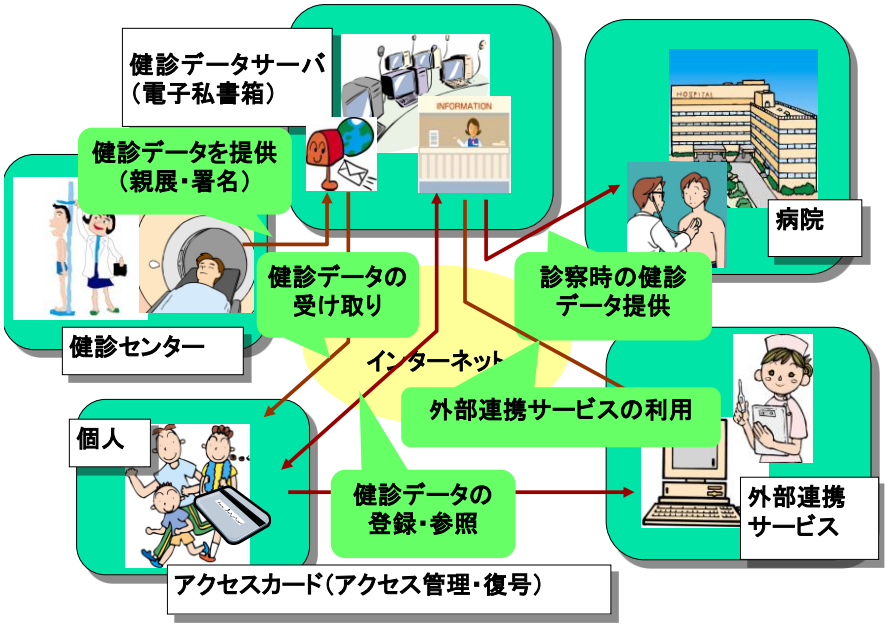


図 6-1　電子私書箱構想による個人健康情報活用システムの概要

6.4　院内連携への適用

XDS は医療施設間同士の情報共有へ応用されることを前提とし応用が多いですが、同一施設内の分散された部門ごとのデータベースを共有する為のツールとしても利用できます。この場合、一人の患者をキーにして、関連した情報が速やかに集約されるインタフェースが必要で、この場合のバックヤードサービスとして XDS を使用することが可能です。利用者からはあたかも一つのデータベースに見えるようにレジストリの検索とリポジトリからのデータの取得を行なえると便利です。

地域医療連携情報システム構築
ハンドブック 2010

―IHE XDS による HIE（Health Information Exchange）の構築―

附属書　参考・解説

附属書 A.　施設間情報連携統合プロファイル XDS　画像連携の場合

本附属書では、IHE XDS の利用場面として画像連携の場合のシステム構築で考慮すべきことを具体例で説明する。

第 6 章でも述べたように、４疾病（がん対策、脳卒中対策、急性心筋梗塞対策、糖尿病対策）及び５事業（救急医療、災害時医療、へき地医療、周産期医療、小児医療）に対する医療計画では、地域医療連携が不可欠となっている。また、医療設備の高度化にともない広域で遠隔地にある施設間の連携の必要性も高まっている。ここでは、放射線医学総合研究所（放医研）におけるがん治療での画像情報を中心にした施設間情報連携の事例を取り上げる。

A.1　構築するシステムのユースケース

「重粒子治療紹介システム」の構築する場合のユースケースを検討してみる。

1) 患者は、具合が悪くなり近医の医療機関 A を受診。結果悪性腫瘍の診断がくだされる。担当医は治療法を挙げて、患者は重粒子治療を選択する。担当医は重粒子治療専門病院に相談することとする。
2) 担当医は、重粒子治療コンサルテーションシステムにアクセスし、コンサルテーション依頼を行う。
3) 放医研相談窓口はコンサルテーション依頼を見て適切な医師に割り振る。
4) 以前のコンサルテーション情報を確認し、同じ患者の履歴があれば同一患者の治療として登録/設定を行う。
5) 医師はコンサルテーション内容（病歴および画像情報）を確認し、治療可否を回答する。同じ患者が過去にコンサルテーション／治療を受けている場合は、同時に過去のコンサルテーション情報／治療情報も参照する。
6) 医療機関 A の担当医は回答を確認し患者に伝える。
7) 重粒子治療可となった場合、患者は紹介状をもって重粒子治療専門病院を受診する。
8) 重粒子治療専門病院では、既存のコンサルテーション内容をふまえ初診を行う。
9) 初診後、重粒子治療専門病院の担当医師は紹介元医師に紹介お礼とともに治療計画や事前の依頼事項を伝える。
10) 患者は重粒子治療専門病院で治療を受ける。
11) 重粒子治療専門病院担当医師は、治療終了後、フォローアップを依頼する施設（紹介元施設とは限らない）へフォロー依頼を行う。依頼時には、治療前の病歴、治療実施情報、治療前検査画像、治療後検査画像等が提供される。
12) フォロー担当医は定期的に患者の状態をチェックし（患者の受診による）、フォローアップ報告を行う。
13) 再発/転移が認められた場合は、再度、重粒子治療の適応を検討する。

A.2　システム構成例

ユースケースを分解し、それぞれの場所で行うべき作業を図 A-1 にまとめる。

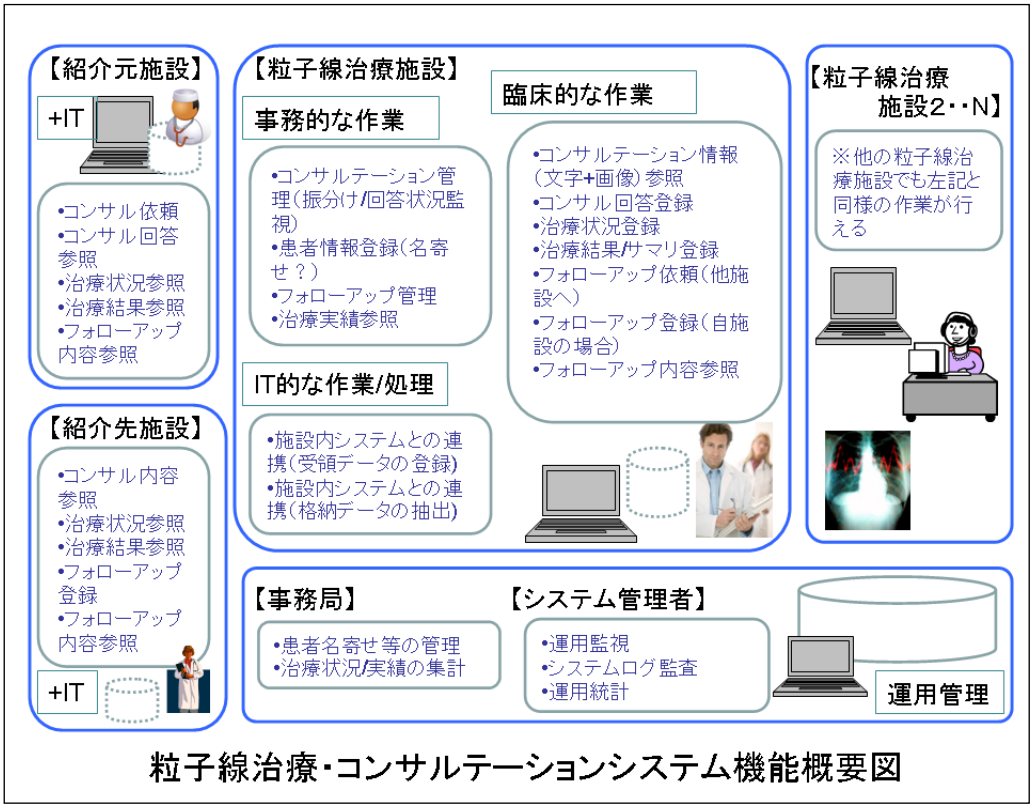


図 A-1　システム構成例

このようにまとめると、システムは大きく分けて４つの機能が必要となることがわかる。

1）患者の文書／画像データを登録する機能
2）患者の文書／画像データを参照する機能
3）文書／画像データを保管・管理する機能
4）システムを運用管理する機能

次のステップでは、これらの処理／機能を実現する IHE の業務シナリオ（統合プロファイル）とアクタを見つけ出せばよい。

A.3　システムと利用する統合プロファイル／アクタ

1）患者の文書／画像データを登録する機能
　① XDS の Document Source
　② XDS-I の Document Image Source
　③ PIX の Patient Identity Source
　④ PIX の Patient Identifier Cross-reference Consumer
　⑤ ATNA の Secure Node

⑥ CT の Time Client

2）患者の文書／画像データを参照する機能
①XDS の Document Consumer
②XDS-I の Document Image Consumer
③PIX の Patient Identifier Cross-reference Consumer
④ATNA の Secure Node
⑤CT の Time Client

3）文書／画像データを保管・管理する機能
① XDS の Document Repository
② XDS の Document Registry

4）システムを運用管理する機能
① ATNA の Audit Record Repository
② CT の Time Server
③ PIX の Patient Identifier Cross-reference Manager
④ PDQ の Patient Demographic Supplier

A.4 仕様書記載ポイント（例）

画像データの交換の場合、画像データの本体をどこに格納・保存するかによりシステム構成が大きく異なる。その構成により仕様書の記載も異なる。ここでは、次のようなシステムを構築するための仕様書例を紹介したい。

＜システム案＞

データ登録：各医療機関
データ参照：各医療機関
文書データ格納：地域連携システムサーバ
画像データ格納：各医療機関の画像サーバ

＜システム・運用例＞

ユースケース概要をもう少しブレイクダウンし、本システムを利用する場面ごとに必要な機能を整理する。

4.1 ユーザ登録＜操作者：紹介元の医師・担当者＞
- コンサルテーションを希望する医療機関の医師は事前に、本コンサルテーションシステムにユーザ登録をする。
- コンサル希望医師は、重粒子医科学センター病院ホームページに掲載する本システムの URL にアクセスし、ユーザ登録申請をする。申請時の入力項目は、医療機関名、所在、電話番号、FAX 番号、医師の所属診療科、医師名（漢字、カナ、ローマ字）等

4.2 ユーザ登録受付＜操作者：コンサルシステム運用管理者＞
- 放医研のコンサルシステム運用管理者は、ユーザ登録申請を受領し、申請内容が正しいことを物理的な手段（電話、郵便、FAX 等）で確認する。

・ ユーザ登録申請の許可ができた場合は、本登録の手続きを行う。

4.3 コンサルテーション依頼＜操作者：紹介元の医師・担当者＞

・ コンサルしたい患者の情報を登録する。登録する情報は、患者基本情報、疾患情報（部位、組織型、TNM、stage)、前治療、現病歴、重複癌有無、依頼内容、画像（直接登録、別途 CD 送付）など。
・ システムから、コンサル番号（以降のキー情報）が発行される。画像を媒体で送付する場合はコンサル内容が印刷できる。

4.4 コンサルテーション振分け＜操作者：放医研の相談窓口担当者＞

・ コンサル状況一覧が表示される。一覧は、依頼日、依頼元、状況（未処理／回答待ち／回答済／医師処理中／医師回答遅延)、疾患情報、回答担当医、画像到着状況などが表示される。
・ “未処理”（＝新規依頼）について、コンサル内容をみて、適切な疾患グループの担当医にコンサル依頼。
・ コンサル内容から以前にも紹介があった患者の場合は、過去情報を検索し過去コンサル歴と関連付けを行い、放医研担当医が容易に両方の情報を参照できるよう設定を行う。
・ “回答遅延”のものは、回答担当医に再度要求する。
・ “回答待ち“のものは、依頼元へ回答担当医の回答と、受診時の必要事項をまとめて送付する。依頼元へは自動的にコンサル番号を基にした回答有等のメールが通知される。

4.5 コンサルテーション依頼内容参照・回答＜操作者：放医研の医師＞

・ コンサル依頼内容をみて、治療適応有無を回答する。
・ 治療適応有（＝放医研で治療可）の場合、治療内容、治療予定、コメント、注意事項等。
・ 治療適応無の場合、理由を回答。

4.6 コンサルテーション回答参照＜操作者：紹介元の医師・担当者＞

・ コンサルテーションシステムにアクセスし回答を参照する。

4.7 受診予約＜操作者：紹介元の医師・担当者＞

・ 患者が希望する場合は、コンサルテーションシステムを利用して初診予約をとる。

4.8 受診＜操作者：放医研の医師＞

・ コンサル番号から、当該患者の病歴情報等を参照する。

4.9 治療 ・・・ 院内電子カルテへの取り込みは次期システムで検討

4.10 フォローアップ依頼＜操作者：放医研の医師＞

・ コンサル番号を元に、治療サマリを記載し、フォローアップを依頼する。
　・・・院内電子カルテ／DB システムから、治療サマリ情報の取得は次期システムで検討。

4.11 フォローアップ登録＜操作者：フォローアップ担当医＞

・ フォローアップ依頼を受けた医療機関は、定期的な患者の受診を契機に、治療のフォローを行う。
・ 治療フォロー時には、医療機関 ID などを元に患者検索を行い、コン

サルテーション番号に対してフォローアップ情報の登録や連絡事項などを記載する。
- フォローアップ情報として登録する項目は、フォローアップ実施日、転帰、副作用（部位ごと）、腫瘍サイズ、再発・再燃有無、画像情報等である。

4.12 再治療依頼＜操作者：フォローアップ担当医＞
- 定期的なフォローアップ時に、腫瘍の再発/転移が認められた場合は、再度コンサルテーションを開始する。このとき、新たにコンサル番号を取得する。

＜システム・仕様書例・抜粋＞

ブレイクダウンしたシナリオを元に、本システムの各機能を設置する場所ごとに必要な要件と機能をまとめる。この時、各システムで実現する IHE の統合プロファイルとアクタを明記することで整理する。ここでは患者の文書／画像データ登録機能について記載する。

1)　患者の文書／画像データを登録する機能

a) コンサルしたい患者の情報を登録する機能を有すること。登録する情報は、患者基本情報、疾患情報（部位、組織型、TNM、stage)、前治療、現病歴、重複癌有無、依頼内容、画像（直接登録、別途 CD 送付）などである。

b) 文書情報の登録は、IHE-IT インフラストラクチャ・XDS 統合プロファイルの Document Source アクタを利用して実現すること。

c) 画像情報の登録は、IHE-IT インフラストラクチャ・XDS-I の Document Image Source アクタを利用して実現すること。

d) 患者情報の登録前に地域連携システム上の患者 ID との整合をとる必要がある。本システムでは地域連携サーバ室に患者情報管理機能が設置されているので、必要な情報を検索し患者が地域連携システムで一意に決まる ID を取得する。地域連携サーバ室にある患者情報管理機能は PIX 統合プロファイルの Patient Identifier Cross-reference Manager アクタ、および PDQ 統合プロファイルの Patient Demographic Supplier アクタを実現する。文書情報登録機能は、PIX の Patient Identity Source アクタおよび Patient Demographic Consumer アクタを実現し、ITI テクニカルフレームワークで指定した通信手順（トランザクション）によって患者情報を取得することとする。

e) 地域連携サーバに登録時には登録した旨を示す監査証跡ログを出力すること。監査証跡ログの出力は、IHE-IT インフラストラクチャ領域の ATNA(Audit Trail and Node Authentication)統合プロファイルの Audit Trail-Secure Node アクタを利用すること。監査証跡ログのイベント ID 等ログ内容の詳細は別途指定したとおりとすること。

f) 正確な情報収集のために、時刻サーバを導入する予定である。文書登録機能は、指定した時刻サーバと時刻同期を行うこと。時刻同期には、ITI-IT インフラストラクチャの CT(Consistent Time)統合プロファイルの Time Client アクタを利用すること。時刻同期は１回／日で実施することとする。実施時間は別途調整する。

附属書 B.　XDS 概論

本附属書では、IHE テクニカルフレームワーク（IHE-ITI-TF-1、2、3 Rev.6）に沿って XDS の技術的な概要を説明する。

現時点においては、XDS は「XDS.a」と「XDS.b」の 2 種類の仕様が存在する。両者の違いは、XDS のベースとなっている ebXML のバージョン、トランザクションの通信方式、　メタデータの属性が一部異なる点などがある。IHE では、今後 XDS.a は XDS.b へ置き換えられ、廃止されることになっている。従って、本書では「XDS.b」の技術的な概要を説明する。以下、「XDS」は「XDS.b」を指すものとする。

なお、実装技術に関しては、附属書 E で具体的なオープンソースの利用方法を紹介する。

B.1　XDS のアクタとトランザクション

XDS は表 B-１に示す５つのアクタ、及び表 B-2 に示す６つのトランザクションから構成される。

表 B-1　XDS を構成するアクタ

アクタ	概要
ドキュメントソース （DocumentSource：文書供給源）	文書（ファイル）および文書のインデックス情報（メタデータ）を提供する。
ドキュメントリポジトリ （DocumentRepository：文書保管庫）	文書そのものを保管する
ドキュメントレジストリ （DocumentRegistry：文書登録簿）	文書のメタデータを保管する
ドキュメントコンシューマ （DocumentConsumer：文書利用者）	文書の検索・参照を行う
患者IDソース （Patient Identity Feed）	患者IDを提供する

表 B-2 XDS で取り扱うトランザクション

トランザクション	概要
Provide and Register Document Set-b [ITI-41]	ドキュメントソースからドキュメントリポジトリへ文書と、そのインデックス情報（メタデータ）を送る。
Register Document Set-b [ITI-42]	ドキュメントリポジトリからドキュメントレジストリへメタデータを登録する。
Registry Stored Query [ITI-18]	検索処理により、ドキュメントコンシューマが、ドキュメントレジストリからメタデータを取り出す。
Retrieve Document Set [ITI-43]	ドキュメントコンシューマが、ドキュメントレジストリから文書を取り出す。
Patient Identity Feed [ITI-8]	ドキュメントレジストリへドメイン内の患者IDの提供を行う（HL7v2形式に基づく）
Patient Identity Feed HL7v3 [ITI-44]	ドキュメントレジストリへドメイン内の患者IDの提供を行う（HL7v3形式に基づく）

XDS におけるアクタとトランザクションの関係は図 B-1 のとおりである。

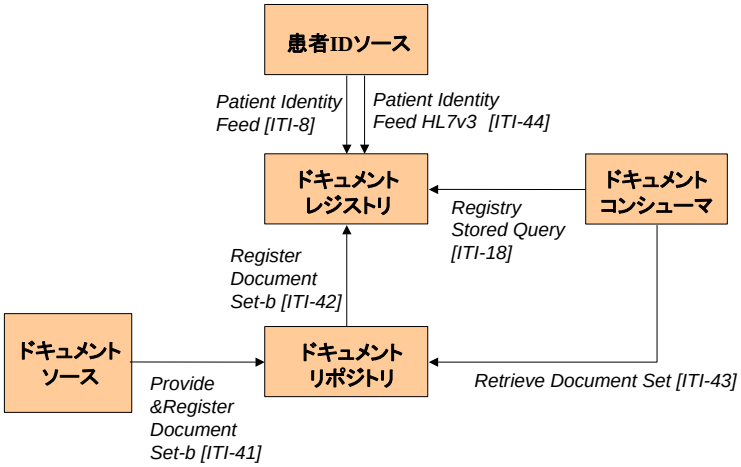


図 B-1 XDS のアクタとトランザクション

なお XDS では、トランザクション、メタデータのスタイルなどで既存の仕様を参照している。XDS に取り入れている既存の仕様を表 B-3 に示す。

表 B-3 XDS の参照仕様[2]

参照技術	使用場面
ebXML ver.3.0	メタデータの記述形式
SOAP1.2	トランザクション間の通信（患者IDソースに関するトランザクションを除く）
MTOM/XOP	トランザクション[ITI-41]、[ITI-43]で文書とメタデータの送信に使用
HL7	患者IDソースから患者IDを供給する、および患者の個人情報をメタデータに記述するときに使用

以後は、ドキュメントソース、ドキュメントリポジトリ、ドキュメントレジストリおよびドキュメントコンシューマは便宜上ソース、リポジトリ、レジストリおよびコンシューマと略する。

この中で患者 ID ソースについては PIX 統合プロファイルで定義されるため、ここでは XDS 固有である他の４つ（ソース、リポジトリ、レジストリ、コンシューマ）を主に説明する。

B.2 XDS における処理の流れ

XDS では主要な処理として「文書[3]・メタデータ登録」「メタデータ検索」「文書の取得」の三つがある。本節では各処理について説明する。

（1）文書・メタデータ登録

ドキュメントソースからドキュメントリポジトリおよびドキュメントレジストリに対して文書およびそのメタデータの登録を実行する。具体的には以下の（イ）（ロ）を順に実行する。

（イ）ソースからリポジトリへの登録要求

(ProvideAndRegisterDocumentSet-b[ITI-41]：図 B-2)

ソースにおいて、リポジトリに登録する文書を１つ以上選定し、文書一つにつき一つのメタデータを作成する。このメタデータは文書に対するインデックス情報となる。文書とそれに対応するメタデータはリポジトリへ送られる。

リポジトリでは、ソースから受け取った文書とメタデータから文書を取り出して保存する。

---

[2]表中に挙げた参照技術の正式名称と参照先は以下の通り。

ebXML：Electronic Business using eXtensible Markup Language、

ebXML レジストリについて http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=regrep を参照

SOAP：Simple Object Access Protocol、 (SOAP1.2) http://www.w3.org/TR/soap12-part0/

MTOM：Message Transmission Optimization Mechanism、http://www.w3.org/TR/soap12-mtom/

XOP：XML-binary Optimized Packaging、http://www.w3.org/TR/xop10/

HL7：Health Level Seven、http;//www.hl7.org/、http://www.hl7.jp

[3]本章における「文書」とは、単なるテキストファイルだけでなく、CDA などの XML 文書、DICOM などの画像なども含めた、コンピュータにおいて一般的に「ファイル」と呼ばれるものすべてを指すものとする。

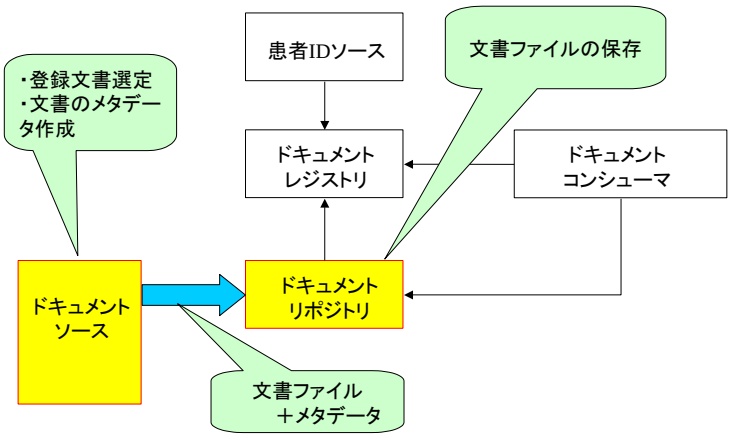


図 B-2 ソースからリポジトリへの登録要求

（ロ）リポジトリからレジストリへの登録要求
（RegisterDocumentSet-b[ITI-42]：図 B-3）

ソースからの登録要求メッセージから文書を取り出し保存した後、リポジトリはその文書の情報（ハッシュ値、サイズ）、及びリポジトリに対して付与されている ID 値（リポジトリ ID）を文書に対応するメタデータに埋め込む。その上でメタデータをレジストリへ送付する。

レジストリでは、リポジトリから受け取ったメタデータを保存する。なお、レジストリにてエラーが発生した場合はその内容をリポジトリ経由でソースへ送る。

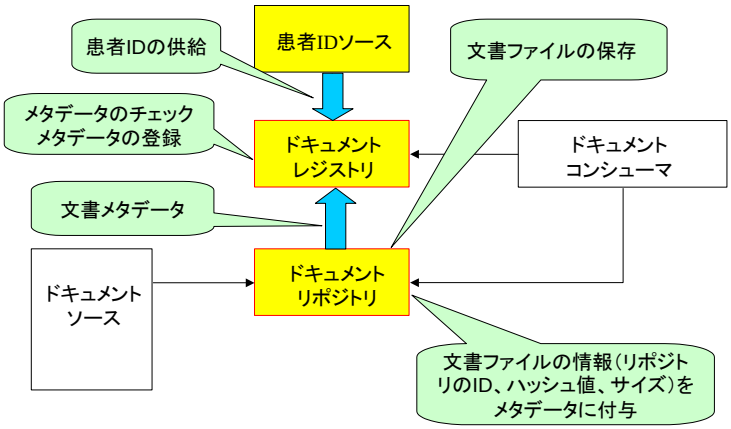


図 B-3 リポジトリからレジストリへの登録要求

（２）メタデータ検索（RegistryStoredQuery[ITI-18]：図 B-4）

コンシューマは、レジストリからメタデータを取得するために、検索条件を含めた検索要求メッセージをレジストリへ送る。

レジストリは検索要求メッセージを受け取ると、検索条件に応じたメタデー

タを検索結果としてコンシューマへ送る。
　コンシューマは検索結果をレジストリから受け取ると、コンシューマ利用者に検索結果を提示する。

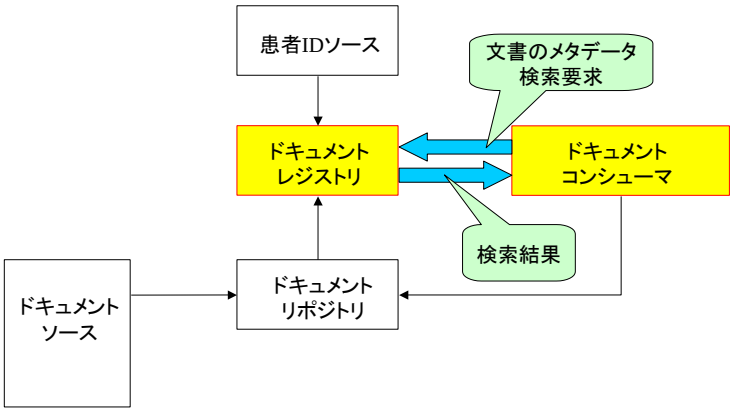


図 B-4　コンシューマからレジストリへの検索要求

　なお、メタデータ検索においてはストアドクエリ(StoredQuery)を利用する。XDS において定義されているストアドクエリの種類を表 B-4 に示す。各クエリの詳細及び定義は ITI-TF-2a の 3.18.4.1.2.3.7 を参照のこと。

表 B-4　XDS におけるストアドクエリの種類

FindDocuments	GetDocument	GetRelatedDocuments	GetSubmissionset
FindFolders	GetSubmissionSetAndContents	GetFolders	
FindSubmissionSets	GetFolderAndContents	GetAssociations	
GetAll	GetFoldersForDocument	GetDocumentsAndAssociations	

（３）文書の取得（RetrieveDocumentSet[ITI-43]：図 B-5）
　前述のメタデータ検索の実行で、取得したい文書のメタデータが得られると、その中に文書がどのリポジトリに存在するかを表す情報（文書所在情報）が含まれている。その情報をもとに、該当のリポジトリに対して文書取得要求メッセージを送る。
　リポジトリは文書取得要求メッセージを受け取ると、要求された文書をコンシューマに送る。コンシューマはリポジトリからの文書を受け取ると、文書の表示などを実行してコンシューマ利用者に提示する。

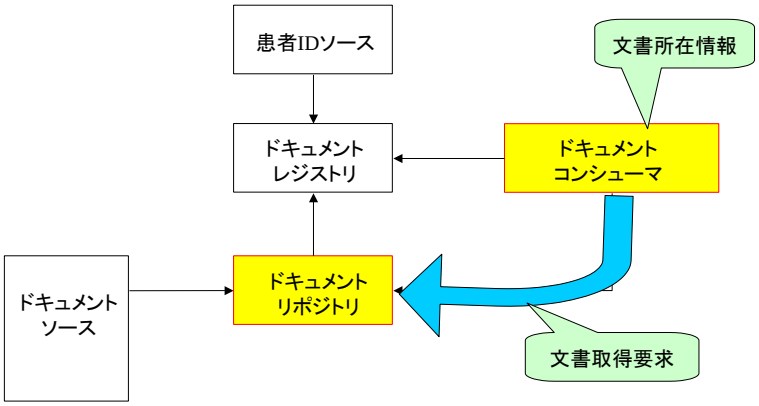


図 B-5 文書の取得要求

B.3 メタデータの種類

XDS で取り扱うメタデータは

- ドキュメントエントリ (DocumentEntry)
- フォルダ (Folder)
- サブミッションセット (SubmissionSet)
- アソシエーション (Association)

の４種類がある。これらはすべてレジストリで管理される。

B.1 節で触れたように、XDS は ebXML の技術をベースにしているため、XDS で取り扱うメタデータを記述するとき、ebXML レジストリ情報モデル(ebXML Registry Information Model: ebXML RIM)ver3.0 の流儀に沿って書く必要がある。ドキュメントエントリは ebXML RIM ver3.0 で定義されている「ExtrinsicObject」として、フォルダ及びサブミッションセットは ebXML RIM ver3.0 での「RegistryPackage」としてそれぞれ記述する。

これらの関係を図 B-6 に示す。フォルダとサブミッションセットはどちらも RegistryPackage を用いて記述するが、両者の区別を付けるために ebXML RIM ver3.0 での「Classification」を利用する。

なおアソシエーションについては ebXML RIM ver3.0 で定義されている「Association」をそのまま取り入れている。

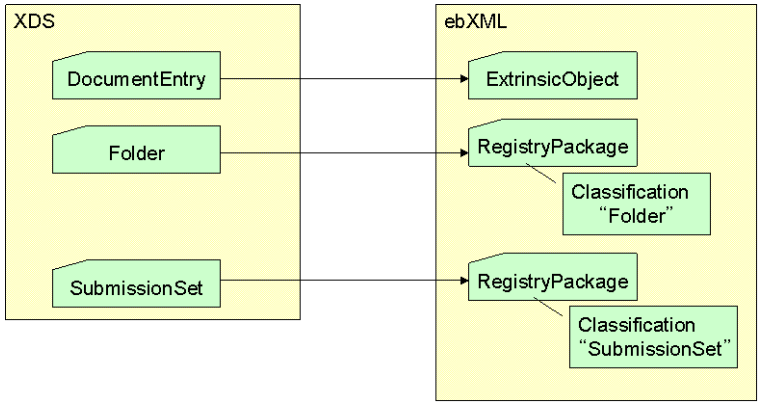


図 B-6 メタデータにおける XDS と ebXML の対応

以下に XDS で取り扱うメタデータが持つ属性の種類を取り上げる。

（1）ドキュメントエントリ（DocumentEntry）

ドキュメントエントリには、リポジトリへ登録する文書のインデックス情報を記述する。

表 B-5 にドキュメントエントリが持つ属性の項目を挙げる。各項目の詳細及び設定方法は ITI-TF-3 の４．１．７を参照のこと。各項目は ebXML RIM ver3.0 で定義されている Slot、Classification、ExternalIdentifier、Name、Description を利用して設定される。

表 B-5 ドキュメントエントリの属性一覧

項目	必要性	項目	必要性
author	R2	homeCommunityId	Cx
authorInstitution	R2	languageCode	R
authorPerson	R2	legalAuthenticator	O
authorRole	R2	mimeType	R
authorSpecialty	R2	patientId	R
availabilityStatus	Cg	practiceSettingCode	R
classCode	R	practiceSettingCodeDisplayName	R
classCodeDisplayName	R	repositoryUniqueId	Cp
comments	O	serviceStartTime	R2
confidentialityCode	R	serviceStopTime	R2
creationTime	R	size	Cp
entryUUID	Cg	sourcePatientId	R
eventCodeList	O	sourcePatientInfo	O
eventCodeDisplayName	O	title	O
formatCode	R	typeCode	R
hash	Cp	typeCodeDisplayName	R
healthcareFacilityCode	R	uniqueId	R
healthcareFacilityCodeDisplayName	R	URI	Cy

凡例 R:必須 R2:明らかであればできるだけ記入する O:任意 Cg:レジストリにて設定(必須)
Cx:レジストリにて設定(必須) Cp:リポジトリにて設定(必須) Cy:リポジトリにて設定(任意)

前述の通り、ドキュメントエントリは ebXML RIM ver.3.0 で定義される

ExtrinsicObject を利用して記述する。以下、図 B-7 にソース側が作成したドキュメントエントリの xml 形式による記述例を示す。

```
<rim:ExtrinsicObject xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
                id="urn:uuid:ee2ed13d-fee6-4239-affa-984c07171ee3"
                mimeType="text/plain" objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1">

 <!-- Slotを使って定義するメタデータ  -- >
 <rim:Slot name="creationTime">
   <rim:ValueList>
     <rim:Value>20051224</rim:Value>
   </rim:ValueList>
 </rim:Slot>
 <rim:Slot name="languageCode">
   <rim:ValueList>
     <rim:Value>en-us</rim:Value>
   </rim:ValueList>
 </rim:Slot>
 <rim:Slot name="sourcePatientId">
   <rim:ValueList>
     <rim:Value>89765a87b^^^&amp;amp;3.4.5&amp;amp;ISO</rim:Value>
   </rim:ValueList>
 </rim:Slot>

 <!– title, comment -- >
 <rim:Name>
   <rim:LocalizedString value="Physical"/>
 </rim:Name>
 <rim:Description/>

 <!-- Classificationを利用して定義するメタデータ -- >
 <rim:Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
                classifiedObject="urn:uuid:ee2ed13d-fee6-4239-affa-984c07171ee3"
                nodeRepresentation="History and Physical“  id="id_3">
   <rim:Slot name="codingScheme">
     <rim:ValueList>
       <rim:Value>Connect-a-thon classCodes</rim:Value>
     </rim:ValueList>
   </rim:Slot>
   <rim:Name>
     <rim:LocalizedString value="History and Physical“ />
   </rim:Name>
 </rim:Classification>
 <!-- 他、confidentialityCode, formatCode, healthcareFacilityTypeCode, practiceSettingCodeが必須だが、
       スペースの関係で省略 -- >

 <!-- ExternalIdentifierを利用して定義するメタデータ -- >
 <rim:ExternalIdentifier identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"
                    value="39a444b558a344c^^^&amp;amp;1.3.6.1.4.1.21367.2005.3.7&amp;amp;ISO"
                    id="id_9"
                    registryObject="urn:uuid:ee2ed13d-fee6-4239-affa-984c07171ee3">
   <rim:Name>
     <rim:LocalizedString value="XDSDocumentEntry.patientId" />
   </rim:Name>
 </rim:ExternalIdentifier>
 <rim:ExternalIdentifier identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
                    value="160.27.80.47.1.40"    id="id_10"
                    registryObject="urn:uuid:ee2ed13d-fee6-4239-affa-984c07171ee3">
   <rim:Name>
     <rim:LocalizedString value="XDSDocumentEntry.uniqueId" />
   </rim:Name>
 </rim:ExternalIdentifier>

</rim:ExtrinsicObject>
```

注: 必要性がR2、Oである属性の内、省略しているものがある。

図 B-7 ドキュメントソース側で作成したドキュメントエントリの例

（2）フォルダ（Folder）

フォルダは目的に応じて複数のドキュメントエントリを束ねるのに用いる。属性の項目一覧を表 B-6 に示す。各属性の詳細は ITI-TF-3 の 4.1.9 を参照のこと。

表 B-6 フォルダの属性一覧

項目	必要性	項目	必要性
availabilityStatus	Cg	homeCommunityId	Cx
codeList	R	lastUpdateTime	Cg
codeListDisplayName	R	patientId	R
comments	O	title	O
entryUUID	Cg	uniqueId	R

凡例 R:必須 R2:明らかであればできるだけ記入する O:任意 Cg:レジストリにて設定(必須)
Cx:レジストリにて設定(任意)

ドキュメントフォルダは、図 B-6 に示すように、ebXML RIM で定義されている RegistryPackage を利用する。またこの RegistryPackage が「フォルダ」であることを示すために、同じ ebXML RIM で定義されている Classification を用いる。図 B-8 にドキュメントフォルダの xml 形式による記述例を示す。

```
<rim:RegistryPackage id="urn:uuid:aae617af-af0f-4a29-979d-8683a8511ba7"
                     xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
  <!-- title, comment -- >
  <rim:Name>
    <rim:LocalizedString value="FOLDER" />
  </rim:Name>
  <rim:Description>
    <rim:LocalizedString value="comments go here" />
  </rim:Description>

  <!-- Classificationを使って定義するメタデータ: codeList -- >
  <rim:Classification classificationScheme="urn:uuid:1ba97051-7806-41a8-a48b-8fce7af683c5"
                  classifiedObject="urn:uuid:aae617af-af0f-4a29-979d-8683a8511ba7"
                  nodeRepresentation="Referrals"  id="id_12">
    <rim:Slot name="codingScheme">
      <rim:ValueList>
        <rim:Value>Connect-a-thon folderCodeList</rim:Value>
      </rim:ValueList>
    </rim:Slot>
    <rim:Name>
      <rim:LocalizedString value="Referrals" />
    </rim:Name>
  </rim:Classification>

  <!-- ExternalIdentifierを利用して定義するメタデータ -- >
  <rim:ExternalIdentifier identificationScheme="urn:uuid:75df8f67-9973-4fbe-a900-df66cefecc5a"
                      value="160.27.80.47.1.53"
                      id="id_13" registryObject="urn:uuid:aae617af-af0f-4a29-979d-8683a8511ba7">
    <rim:Name>
      <rim:LocalizedString value="XDSFolder.uniqueId" />
    </rim:Name>
  </rim:ExternalIdentifier>
  <rim:ExternalIdentifier identificationScheme="urn:uuid:f64ffdf0-4b97-4e06-b79f-a52b38ec2f8a"
                      value="39a444b558a344c^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO"
                      id="id_14"  registryObject="urn:uuid:aae617af-af0f-4a29-979d-8683a8511ba7">
    <rim:Name>
      <rim:LocalizedString value="XDSFolder.patientId" />
    </rim:Name>
  </rim:ExternalIdentifier>
</rim:RegistryPackage>

<!-- 上記RegistryPackageが「フォルダ」であることを定義するClassification。RegistryPackage内に入れてもよい -- >
<rim:Classification xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
                  classifiedObject="urn:uuid:aae617af-af0f-4a29-979d-8683a8511ba7"
                  classificationNode="urn:uuid:d9d542f3-6cc4-48b6-8870-ea235fbc94c2"
                  id="urn:uuid:307875ac-c587-490f-af9e-ba0a46769b62" >
</rim:Classification>
```

図 B-8　ドキュメントソース側で作成するドキュメントフォルダの例

（3）サブミッションセット（SubmissionSet）

サブミッションセットは、ドキュメントをレジストリに登録（提供）する際のドキュメントエントリおよびフォルダに関する情報を含むメタデータの集合を表す。サブミッションセットは一回の登録につき、必ず一つ必要となる。

表 B-7 にサブミッションセットの属性項目一覧を示す。また各属性の詳細は ITI-TF-3 の 4.1.8 を参照のこと。

表 B-7 サブミッションセットの属性一覧

項目	必要性	項目	必要性
author	R2	entryUUID	Cg
authorInstitution	R2	homeCommunityId	Cx
authorPerson	O	intendedRecipient	O
authorRole	R2	patientId	R
authorSpecialty	R2	sourceId	R
availabilityStatus	Cg	submissionTime	R
comments	O	title	O
contentTypeCode	R	uniqueId	R
contentTypeCodeDisplayName	R		

凡例 R:必須 R2:明らかであればできるだけ記入する O:任意 Cg:レジストリにて設定(必須)
Cx:レジストリにて設定(任意)

サブミッションセットは、図 B-6 に示すように、ebXML RIM で定義されている RegistryPackage を利用する。またこの RegistryPackage が「サブミッションセット」であることを示すために、同じ ebXML RIM で定義されている Classification を用いる。図 B-9 にサブミッションセットの xml 形式による記述例を示す。

```
<rim:RegistryPackage id="urn:uuid:a83d67b2-210b-41ac-80e4-9c81c6b16d26"
                     xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">

 <!-- Slotを利用して定義するメタデータ-- >
 <rim:Slot name="submissionTime">
  <rim:ValueList>
   <rim:Value>20041225235050</rim:Value>
  </rim:ValueList>
 </rim:Slot>

 <!-- title,comment -- >
 <rim:Name>
  <rim:LocalizedString value="Physical" />
 </rim:Name>
 <rim:Description>
  <rim:LocalizedString value="Annual physical" />
 </rim:Description>

 <!-- Classificationを利用して定義するメタデータ -- >
 <rim:Classification classificationScheme="urn:uuid:aa543740-bdda-424e-8c96-df4873be8500"
                     classifiedObject="urn:uuid:a83d67b2-210b-41ac-80e4-9c81c6b16d26"
                     nodeRepresentation="History and Physical" id="id_16">
  <rim:Slot name="codingScheme">
   <rim:ValueList>
    <rim:Value>Connect-a-thon contentTypeCodes</rim:Value>
   </rim:ValueList>
  </rim:Slot>
  <rim:Name>
   <rim:LocalizedString value="History and Physical"/>
  </rim:Name>
 </rim:Classification>

 <!-- ExternalIdetifierを利用して定義するメタデータ -- >
 <rim:ExternalIdentifier identificationScheme="urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8"
                         value="160.27.80.47.1.52"
                         id="id_17" registryObject="urn:uuid:a83d67b2-210b-41ac-80e4-9c81c6b16d26">
  <rim:Name>
   <rim:LocalizedString value="XDSSubmissionSet.uniqueId"/>
  </rim:Name>
 </rim:ExternalIdentifier>
 <rim:ExternalIdentifier identificationScheme="urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832"
                         value="1.3.6.1.4.1.21367.2009.1.&#xD;&#xA;d02&#xD;&#xA;2.1"
                         id="id_18" registryObject="urn:uuid:a83d67b2-210b-41ac-80e4-9c81c6b16d26">
  <rim:Name>
   <rim:LocalizedString value="XDSSubmissionSet.sourceId"/>
  </rim:Name>
 </rim:ExternalIdentifier>
 <rim:ExternalIdentifier identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446"
                         value="39a444b558a344c^^^&amp;1.3.6.1.4.1.21367.2005.3.7&amp;ISO"
                         id="id_19" registryObject="urn:uuid:a83d67b2-210b-41ac-80e4-9c81c6b16d26">
  <rim:Name>
   <rim:LocalizedString value="XDSSubmissionSet.patientId"/>
  </rim:Name>
 </rim:ExternalIdentifier>
</rim:RegistryPackage>

<!-- 上記RegistryPackageが「サブミッションセット」であることを定義するClassification。RegistryPackage内で入れてもよい -- >
<rim:Classification xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
                    classifiedObject="urn:uuid:a83d67b2-210b-41ac-80e4-9c81c6b16d26"
                    classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd"
                    id="urn:uuid:895fbb6f-dc68-46a6-81c2-b340a1b53e77" >
</rim:Classification>
```

注： 必要性がR2、Oである属性の内、省略しているものがある。

図 B-9 ドキュメントソース側で作成するサブミッションセットの例

（4）コードの定義

上記（1）～（3）で説明したメタデータの属性の中には、あらかじめ定義されたコードの中から選択して決めるものがある。ドキュメントエントリの classCode、フォルダの codeList、サブミッションセットの contentTypeCode など、属性名に「Code」を含み、ebXMLRIM の Classification を利用して設定される属性がこれに当たる。コードの定義は XDS アフィニティドメインの一部として定義される。一例として、図 B-10 にドキュメントエントリで設定される confidentialityCode の定義例を示す。また、IHE のサイト[4]及び JAHIS の技術文書[5]からもコードの定義を参照することができる。

```
<CodeType name="confidentialityCode" classScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f">
  <Code code="N" display="Normal" codingScheme="2.16.840.1.113883.5.25"/>
  <Code code="R" display="Restricted" codingScheme="2.16.840.1.113883.5.25"/>
  <Code code="V" display="very restricted" codingScheme="2.16.840.1.113883.5.25"/>
  <Code code="C" display="Celebrity" codingScheme="Connect-a-thon confidentialityCodes"/>
  <Code code="D" display="Clinician" codingScheme="Connect-a-thon confidentialityCodes"/>
  <Code code="I" display="Individual" codingScheme="Connect-a-thon confidentialityCodes"/>
  <Code code="N" display="Normal" codingScheme="Connect-a-thon confidentialityCodes"/>
  <Code code="R" display="Restricted" codingScheme="Connect-a-thon confidentialityCodes"/>
  <Code code="S" display="Sensitive" codingScheme="Connect-a-thon confidentialityCodes"/>
  <Code code="T" display="Taboo" codingScheme="Connect-a-thon confidentialityCodes"/>
</CodeType>
```

図 B-10 confidentialityCode の定義例

（5）アソシエーション（Association）

アソシエーションはメタデータ間の関連を表す。これは ebXML RIM で定義された「Association」をそのまま利用する。

表 B-8 アソシエーションの属性一覧

項目	必要性
id	Cg
sourceObject	R
targetObject	R
associationType	R

凡例 R:必須
Cg:レジストリにて設定

アソシエーションは以下の場面で使用する。

- フォルダによるドキュメントエントリ集合構築
- サブミッションセットを用いた登録単位の作成

3 http://ihexds.nist.gov/xdsref/codes/codes.xml

4「地域医療連携システム　診察情報共有化のための IHE XDS 適用ガイド」（JAHIS 技術文書 09-101）の 7.章参照　http://www.jahis.jp/standard/seitei/st09-101v1.0a/st09-101v1.0a.pdf

・ ドキュメント間の関連

以下、これらを順に説明する。

・フォルダによるドキュメントエントリ集合構築

上述（２）で述べたとおり、フォルダは複数のドキュメントエントリを束ねるのに利用されるが、その際にアソシエーションを利用する。図 B-11 はその一例である。

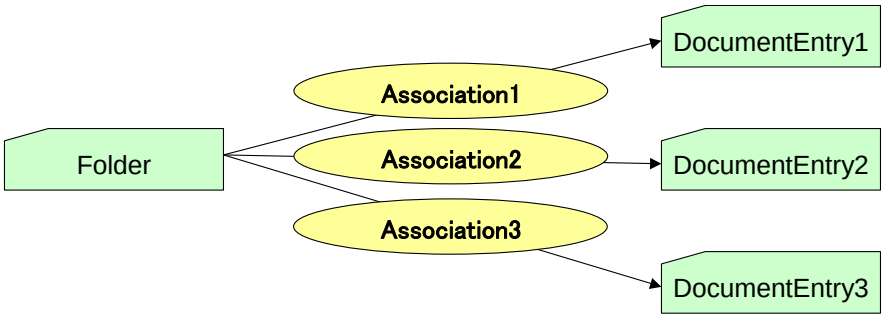


図 B-11 フォルダによるドキュメントエントリ集合の例

この場合、各アソシエーションの属性値はそれぞれ以下のように設定する（表 B-9、図 B-12）。

表 B-9 属性値の設定

項目	値
sourceObject	FolderのentryUUID
targetObject	(Association1の場合)DocumentEntry1のentryUUID (Association2の場合)DocumentEntry2のentryUUID (Association3の場合)DocumentEntry3のentryUUID
associationType	urn:oasis:names:tc:ebxml-regrep:AssocaitionType:HasMember

```
<rim:Association id="Association1のid"
                associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember"
                sourceObject="FolderのentryUUID"
                targetObject="DocumentEntry1のentryUUID" >
</rim:Association>
<rim:Association id="Association2のid"
                associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember"
                sourceObject="FolderのentryUUID"
                targetObject="DocumentEntry2のentryUUID" >
</rim:Association>
<rim:Association id="Association3のid"
                associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember"
                sourceObject="FolderのentryUUID"
                targetObject="DocumentEntry3のentryUUID" >
</rim:Association>
```

図 B-12　アソシエーション設定例

・サブミッションセットを用いた登録単位の作成

上述（３）で述べたように、サブミッションセットは、ドキュメントをレジストリに登録（提供）する際のドキュメントエントリおよびフォルダに関する情報を含むメタデータの集合を表す。この集合を構成するのにアソシエーションを利用する。この場合、サブミッションセットと他のメタデータとのアソシエーションが持つ属性値は次のようになる（表 B-10）。

表 B-10　属性値の設定

項目	値
sourceObject	サブミッションセットのentryUUID
targetObject	ドキュメントエントリ、フォルダのentryUUID、 あるいはフォルダ、ドキュメントエントリ間サブミッションセットのid
associationType	urn:oasis:names:tc:ebxml-regrep:AssocaitionType:HasMember

図 B-13 に例を示す。

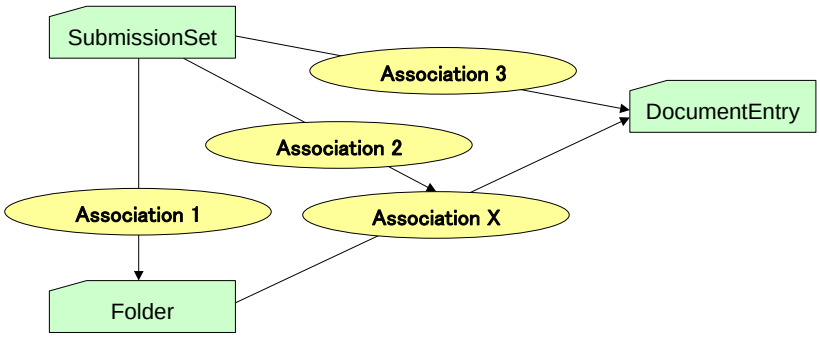


図 B-13　サブミッションセットを利用した登録単位の例

本例において、Association1 から Association3 の属性値はそれぞれ以下の値

をとる。

表 B-11 属性値の設定

項目	値
sourceObject	SubmissionSetのentryUUID
targetObject	(Assoxiation1の場合)FolderのentryUUID (Assocaition2の場合)AssociationXのid (Association3の場合)DocumentEntryのentryUUID
associationType	urn:oasis:names:tc:ebxml-regrep:AssocaitionType:HasMember

・ドキュメント間の関連

XDS では２つの文書の関係を定義できる。具体的には文書に対するドキュメントエントリとの間の関係を、アソシエーションを利用して定義するもので、定義可能な関係は以下のとおり。

表 B-12 文書間関係

文書間関係	説明
差し替え (Replacement：RPLC)	targetObjectで指定した文書を、sourceObjectで指定した文書に差し替える
添付 (Addendum：APND)	targetObjectで指定した文書に、sourceObjectで指定した文書を追加する
変換 (Transformation：XFRM)	sourceObjectで指定した文書はtargetObjectで指定した文書を(翻訳などを行って)変換したものを表す。
変換・差し替え (Transformation-Replacement：XFRM_RPLC)	sourceObjectで指定した文書はtargetObjectで指定した文書を(翻訳などを行って)変換したものであり、かつtargetObjectで指定した文書を、sourceObjectで指定した文書に差し替える。
署名 (signs)	sourceObjectで指定した文書はtargetObjectで指定した文書の電子署名であることを表す。

表 B-13 文書間関係と associationType での設定値

文書間関係	associationTypeでの設定値
差し替え(RPLC)	urn:ihe:iti:2007:AssociationType:RPLC
添付(APND)	urn:ihe:iti:2007:AssociationType:APND
変換(XFRM)	urn:ihe:iti:2007:AssociationType:XFRM
変換・差し替え(XFRM_RPLC)	urn:ihe:iti:2007:AssociationType:XFRM_RPLC
署名(signs)	urn:ihe:iti:2007:AssociationType:signs

図 B-14 に例を示す。本例では２つのドキュメントエントリ DocumentEntry1 と DocumentEntry2 があり、DocumentEntry1 は既にレジストリへ登録されていて、これを「差し替える」ために DocumentEntry2 を登録する。

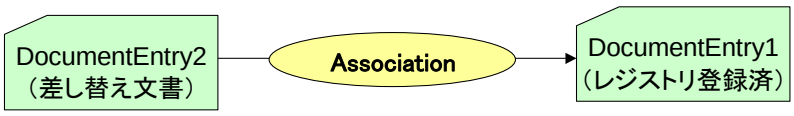


図 B-14　2つの文書の対応関係（差し替え）の例

この場合、アソシエーションの各属性は以下のようになる（表 B-14）。

表 B-14 各属性の設定値

項目	値
sourceObject	DocumentEntry2のentryUUID
targetObject	DocumentEntry1のentryUUID
associationType	urn:ihe:iti:2007:AssociationType:RPLC

なお、文書の差し替えでは、差し替えられた文書（上記の例では DocumentEntry1）の属性 availabilityStatus の値がレジストリ側で変更される。このように文書間関連の設定においては、表 B-12 に定義した関係に応じて追加で行うべき処理が存在する。文書間関連の詳細については ITI-TF-3 の 4.1.6 項を参照のこと。

B.4　トランザクションの通信方式

XDS を構成するソース、リポジトリ、レジストリ及びコンシューマの各アクタ間のトランザクションでは、通信の方式として SOAP1.2 を採用している。さらに文書本体を取り扱う[ITI-41]と[ITI-43]では、SOAP1.2 に加え MTOM/XOP（MTOM with XOP encoding）形式を利用することが ITI-TF-2b において規定されている（3.41.5 及び 3.43.5 を参照）。各トランザクションの通信方式を図示したのが図 B-15 である。

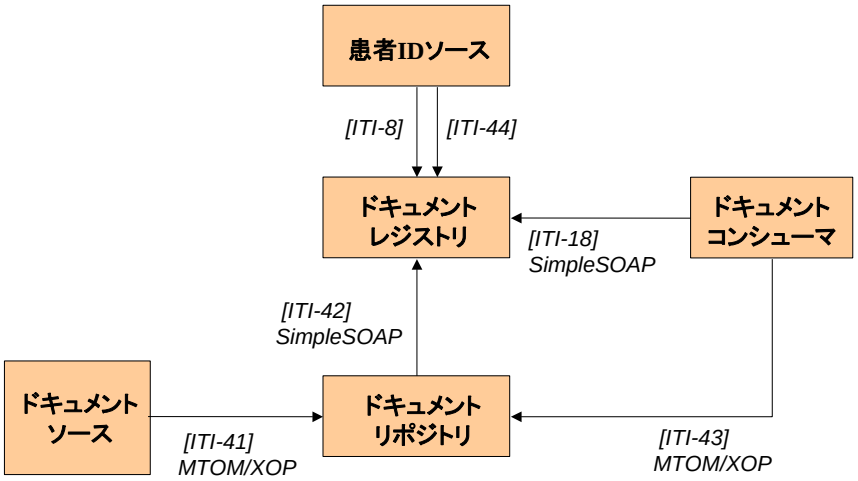


図 B-15 トランザクションの通信方式

以下、各トランザクションで取り扱われる SOAP メッセージの例を示す。

（1）文書・メタデータ登録[ITI-41]

ソースからリポジトリに対して出される文書登録要求の例を図 B-16 に、その要求例に対する返信メッセージを図 B-17 に示す。文書登録要求だけでなく、要求に対する返信メッセージも MTOM/XOP 形式を利用した SOAP メッセージであることに注意すること。

本例はソースから 1 つの文書を登録する場合の SOAP メッセージを表している。そのためメタデータとして、ドキュメントエントリ、サブミッションセット、アソシエーションが一つずつ SOAP メッセージの Body 部に入っている(ただし、図 B-16 では Slot、Classification、ExternalIdentifier で記述されるメタデータの属性値を省略している)

また、SOAP メッセージの Body 部の下部に Document タグがあるが、これは文書本体とその文書のドキュメントエントリとの対応を記述する。文書本体は SOAP メッセージの添付データとして取り扱われる。

また、図 B-17 のメッセージは登録が成功した場合の返信メッセージである。これはメッセージ中の RegistryResponse タグに含まれる属性値 status が Success であることからわかる（図 B-17 の赤字部分）もし、エラーが発生して登録が失敗した場合は、この属性値が Failure となり、SOAP の Body 部にエラーの内容が記載されている。

```
POST /tf6/services/xdsrepositoryb HTTP/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_82378215884CFDAF4E1268820255283;
type="application/xop+xml"; start="<0.urn:uuid:82378215884CFDAF4E1268820255284@apache.org>";
start-info="application/soap+xml"; action="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b"
User-Agent: Axis2
Host: jiji:9080
Transfer-Encoding: chunked

--MIMEBoundaryurn_uuid_82378215884CFDAF4E1268820255283
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:82378215884CFDAF4E1268820255284@apache.org>

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
            xmlns:wsa="http://www.w3.org/2005/08/addressing">
 <soapenv:Header>
  <wsa:To>http://elektra:9080/tf6/services/xdsrepositoryb</wsa:To>
  <wsa:MessageID>urn:uuid:82378215884CFDAF4E1268820254957</wsa:MessageID>
  <wsa:Action>urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b</wsa:Action>
 </soapenv:Header>
 <soapenv:Body>
  <xdsb:ProvideAndRegisterDocumentSetRequest xmlns:xdsb="urn:ihe:iti:xds-b:2007">
   <lcm:SubmitObjectsRequest xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0">
    <rim:RegistryObjectList xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">

     <rim:ExtrinsicObject id="urn:uuid:7a4fc48b-8d20-462a-a8a7-8b94076780eb"
         mimeType="text/plain"
         objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1">
      <!-- 省略-- >
     </rim:ExtrinsicObject>
     <rim:RegistryPackage id="urn:uuid:a83d67b2-210b-41ac-80e4-9c81c6b16d26">
      <!-- 省略-- >
     </rim:RegistryPackage>
     <rim:Classification classifiedObject="urn:uuid:a83d67b2-210b-41ac-80e4-9c81c6b16d26"
                 classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd"
                 id="urn:uuid:895fbb6f-dc68-46a6-81c2-b340a1b53e77">
     </rim:Classification>
     <rim:Association associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember"
                 sourceObject="urn:uuid:a83d67b2-210b-41ac-80e4-9c81c6b16d26"
                 targetObject="urn:uuid:7a4fc48b-8d20-462a-a8a7-8b94076780eb"
                 id="urn:uuid:edc81ecc-d5e8-4eca-a1b7-d3f4c89e41db">
     </rim:Association>

    </rim:RegistryObjectList>
   </lcm:SubmitObjectsRequest>

   <xdsb:Document id="urn:uuid:7a4fc48b-8d20-462a-a8a7-8b94076780eb">
    <xop:Include href="cid:1.urn:uuid:82378215884CFDAF4E1268820255652@apache.org"
        xmlns:xop="http://www.w3.org/2004/08/xop/include" />
   </xdsb:Document>

  </xdsb:ProvideAndRegisterDocumentSetRequest>
 </soapenv:Body>
</soapenv:Envelope>

--MIMEBoundaryurn_uuid_82378215884CFDAF4E1268820255283
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:82378215884CFDAF4E1268820255652@apache.org>

This is my document.

It is great!


--MIMEBoundaryurn_uuid_82378215884CFDAF4E1268820255283--
```

メタデータ

文書本体へのポインタ

文書本体

図 B-16 ドキュメントソースからの文書登録要求メッセージ

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related; boundary=MIMEBoundaryurn_uuid_D93C36CAA0149E1BB01268820290558;
type="application/xop+xml"; start="0.urn:uuid:D93C36CAA0149E1BB01268820290559@apache.org";
start-info="application/soap+xml"; action="urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-bResponse"
Transfer-Encoding: chunked
Date: Wed, 17 Mar 2010 10:04:50 GMT

--MIMEBoundaryurn_uuid_D93C36CAA0149E1BB01268820290558
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:D93C36CAA0149E1BB01268820290559@apache.org>

<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
                  xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <soapenv:Header>
    <wsa:Action>urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-bResponse</wsa:Action>
    <wsa:RelatesTo>urn:uuid:82378215884CFDAF4E1268820254957</wsa:RelatesTo>
  </soapenv:Header>
  <soapenv:Body>
    <rs:RegistryResponse xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
                         status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" />
  </soapenv:Body>
</soapenv:Envelope>

--MIMEBoundaryurn_uuid_D93C36CAA0149E1BB01268820290558--
```

図 B-17 ドキュメントレジストリからの返信メッセージ

（2）メタデータの登録［ITI-42］

リポジトリからレジストリに対して出されるメタデータ登録要求の例を図 B-18 に、その要求例に対する返信メッセージを図 B-19 に示す。メタデータの登録要求及びその返信メッセージは、MTOM/XOP を用いない通常の SOAP メッセージを利用する。

本例は、リポジトリがソースからの 1 つの文書を登録する要求を受け取り、その中に含まれるメタデータを取り出して文書に関する追加情報（図 B-18 の中央部参照）を付与し、レジストリにこれらのメタデータを登録しようというものである。そのため SOAP メッセージの Body 部にドキュメントエントリ、サブミッションセット、アソシエーションが各 1 つ含まれている（ただし、図 B-18 ではメタデータの属性値を省略している）。

また、図 B-19 のメッセージは登録が成功した場合の返信メッセージである。これはメッセージ中の RegistryResponse タグに含まれる属性値 status が Success であることからわかる（図 B-19 の赤字部分）もし、エラーが発生して登録が失敗した場合は、この属性値が Failure となり、SOAP の Body 部にエラーの内容が記載されている。

```
POST /tf6/services/xdsregistryb HTTP/1.1
Content-Type: application/soap+xml; charset=UTF-8; action="urn:ihe:iti:2007:RegisterDocumentSet-b"
User-Agent: Axis2
Host: jiji:9080
Transfer-Encoding: chunked

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
            xmlns:wsa="http://www.w3.org/2005/08/addressing">
 <soapenv:Header>
  <wsa:To>http://elektra:9080/tf6/services/xdsregistryb</wsa:To>
  <wsa:MessageID>urn:uuid:48F456C97F7F86E4421268909398104</wsa:MessageID>
  <wsa:Action>urn:ihe:iti:2007:RegisterDocumentSet-b</wsa:Action>
 </soapenv:Header>
 <soapenv:Body>
  <lcm:SubmitObjectsRequest xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0">
   <rim:RegistryObjectList xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
    <rim:ExtrinsicObject id="Document01" mimeType="text/plain"
                 objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1">
     <rim:Slot name="repositoryUniqueId">
      <rim:ValueList>
       <rim:Value>1.19.6.24.109.42.1</rim:Value>
      </rim:ValueList>
     </rim:Slot>
     <rim:Slot name="size">
      <rim:ValueList>
       <rim:Value>4</rim:Value>
      </rim:ValueList>
     </rim:Slot>
     <rim:Slot name="hash">
      <rim:ValueList>
       <rim:Value>e543712c0e10501972de13a5bfcbe826c49feb75</rim:Value>
      </rim:ValueList>
     </rim:Slot>
     <!-- 他の属性は省略 -- >
    </rim:ExtrinsicObject>
    <rim:RegistryPackage id="SubmissionSet01" >
     <!-- 省略 -- >
    </rim:RegistryPackage>
    <rim:Classification classifiedObject="SubmissionSet01"
                 classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd"
                 id="ID_16164678_1">
    </rim:Classification>
    <rim:Association associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember"
                 sourceObject="SubmissionSet01"
                 targetObject="Document01"
                 id="ID_16164678_2" >
    </rim:Association>
   </rim:RegistryObjectList>
  </lcm:SubmitObjectsRequest>
 </soapenv:Body>
</soapenv:Envelope>
```

リポジトリで追加された属性

メタデータ

図 B-18 ドキュメントリポジトリからのメタデータ登録要求

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/soap+xml; action="urn:ihe:iti:2007:RegisterDocumentSet-bResponse";charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 18 Mar 2010 10:49:59 GMT

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
                  xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <soapenv:Header>
    <wsa:Action>urn:ihe:iti:2007:RegisterDocumentSet-bResponse</wsa:Action>
    <wsa:RelatesTo>urn:uuid:48F456C97F7F86E44212689093981O4</wsa:RelatesTo>
  </soapenv:Header>
  <soapenv:Body>
    <rs:RegistryResponse xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
                         status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" />
  </soapenv:Body>
</soapenv:Envelope>
```

図 B-19 ドキュメントレジストリからの返信メッセージ

（３）メタデータ検索要求［ITI-18］

コンシューマからレジストリに対して出されるメタデータ検索要求メッセージの例を図 B-20 に、検索要求の例に対する結果（検索結果）のメッセージを図 B-21 にそれぞれ示す。検索要求及び検索結果は、MTOM/XOP を用いない通常の SOAP メッセージを利用する。

先に触れたとおり、メタデータ検索要求はストアドクエリを利用する。本例では、ストアドクエリ「GetDocument」に基づくもので、検索条件は uniqueId が「160.27.80.47.54」あるいは「160.27.80.47.55」であるドキュメントエントリであることを意味する（図 B-20 中にある name が「$XDSDocumentEntryUniqueId」である Slot オブジェクトが検索条件を表す）。

図 B-21 に示す検索結果には、検索により見つかった、uniqueId が「160.27.80.47.54」であるドキュメントエントリと uniqueId が「160.27.80.47.55」であるドキュメントエントリの 2 つが含まれている（ただし、図 B-21 では uniqueId 以外のドキュメントエントリの属性値を省略している）。

```
POST /tf6/services/xdsregistryb HTTP/1.1
Content-Type: application/soap+xml; charset=UTF-8; action="urn:ihe:iti:2007:RegistryStoredQuery"
User-Agent: Axis2
Host: jiji:9080
Transfer-Encoding: chunked

<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
                  xmlns:wsa="http://www.w3.org/2005/08/addressing">
 <soapenv:Header>
  <wsa:To>http://elektra:9080/tf6/services/xdsregistryb</wsa:To>
  <wsa:MessageID>urn:uuid:6C0A7AC4D92351F45B1268908706961</wsa:MessageID>
  <wsa:Action>urn:ihe:iti:2007:RegistryStoredQuery</wsa:Action>
 </soapenv:Header>
 <soapenv:Body>
  <query:AdhocQueryRequest xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
                           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                           xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
                           xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
   <query:ResponseOption returnComposedObjects="true" returnType="LeafClass" />
   <AdhocQuery id="urn:uuid:5c4f972b-d56b-40ac-a5fc-c8ca9b40b9d4">
    <Slot name="$XDSDocumentEntryUniqueId">
     <ValueList>
      <Value>('160.27.80.47.1.54','160.27.80.47.1.55')</Value>
     </ValueList>
    </Slot>
   </AdhocQuery>
  </query:AdhocQueryRequest>
 </soapenv:Body>
</soapenv:Envelope>
```

図 B-20 ドキュメントレジストリへの検索要求

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/soap+xml; action="urn:ihe:iti:2007:RegistryStoredQueryResponse";charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 18 Mar 2010 10:38:28 GMT

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
                  xmlns:wsa="http://www.w3.org/2005/08/addressing">
 <soapenv:Header>
  <wsa:Action>urn:ihe:iti:2007:RegistryStoredQueryResponse</wsa:Action>
  <wsa:RelatesTo>urn:uuid:6C0A7AC4D92351F45B1268908706961</wsa:RelatesTo>
 </soapenv:Header>
 <soapenv:Body>
  <query:AdhocQueryResponse xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
                            status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
   <rim:RegistryObjectList xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">

    <rim:ExtrinsicObject id="urn:uuid:5d57a8e7-fa67-4d08-bc88-d3fdd41036ba"
                         objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
                         status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved"
                         mimeType="text/plain" isOpaque="false" home=""
                         lid="urn:uuid:5d57a8e7-fa67-4d08-bc88-d3fdd41036ba">
     <!-- 省略 -- >
     <rim:ExternalIdentifier id="urn:uuid:5a7acd13-3ef7-46e7-8e80-a0af73fbe9d0"
              objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:ExternalIdentifier"
              identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
              value="160.27.80.47.1.54"
              home="" lid="urn:uuid:5a7acd13-3ef7-46e7-8e80-a0af73fbe9d0"
              registryObject="urn:uuid:5d57a8e7-fa67-4d08-bc88-d3fdd41036ba">
      <rim:Name>
       <rim:LocalizedString xml:lang="en-us" charset="UTF-8" value="XDSDocumentEntry.uniqueId" />
      </rim:Name>
      <rim:Description />
      <rim:VersionInfo versionName="1.1" />
     </rim:ExternalIdentifier>
    </rim:ExtrinsicObject>

    <rim:ExtrinsicObject id="urn:uuid:427a40e6-7214-425a-a020-ed83192b88ac"
                         objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
                         status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved"
                         mimeType="text/plain" isOpaque="false" home=""
                         lid="urn:uuid:427a40e6-7214-425a-a020-ed83192b88ac">
     <!-- 省略 -- >
     <rim:ExternalIdentifier id="urn:uuid:df573256-0d32-44bc-8954-be0123b5fba7"
              objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:ExternalIdentifier"
              identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
              value="160.27.80.47.1.55"
              home="" lid="urn:uuid:df573256-0d32-44bc-8954-be0123b5fba7"
              registryObject="urn:uuid:427a40e6-7214-425a-a020-ed83192b88ac">
      <rim:Name>
       <rim:LocalizedString xml:lang="en-us" charset="UTF-8" value="XDSDocumentEntry.uniqueId" />
      </rim:Name>
      <rim:Description />
      <rim:VersionInfo versionName="1.1" />
     </rim:ExternalIdentifier>
    </rim:ExtrinsicObject>

   </rim:RegistryObjectList>
  </query:AdhocQueryResponse>
 </soapenv:Body>
</soapenv:Envelope>
```

図 B-21 レジストリからの検索結果

（４）文書の取得［ITI-43］

コンシューマからリポジトリへ出される文書取得要求メッセージの例を図 B-22 に、このメッセージ例に対する結果として得られる文書取得結果メッセージの例を図 B-23 にそれぞれ示す。文書取得要求メッセージと文書取得結果メッセージは両方とも MTOM/XOP 形式を利用した SOAP メッセージであることに注意すること。

文書取得要求では、取得したい文書があるリポジトリの uniqueId（repositoryUniqueId）と取得したい文書の uniqueId をメッセージ内で指定する（図 B-22 の下部にある DocumentRequest タグを参照）

```
POST /tf6/services/xdsrepositoryb HTTP/1.1
Content-Type: multipart/related;
boundary=MIMEBoundaryurn_uuid_6C0A7AC4D92351F45B1268908711218;
type="application/xop+xml";
start="<0.urn:uuid:6C0A7AC4D92351F45B1268908711219@apache.org>";
start-info="application/soap+xml"; action="urn:ihe:iti:2007:RetrieveDocumentSet"
User-Agent: Axis2
Host: jiji:9080
Transfer-Encoding: chunked

--MIMEBoundaryurn_uuid_6C0A7AC4D92351F45B1268908711218
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:6C0A7AC4D92351F45B1268908711219@apache.org>

<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
                  xmlns:wsa="http://www.w3.org/2005/08/addressing">
 <soapenv:Header>
  <wsa:To>http://elektra:9080/tf6/services/xdsrepositoryb</wsa:To>
  <wsa:MessageID>urn:uuid:6C0A7AC4D92351F45B1268908711215</wsa:MessageID>
  <wsa:Action>urn:ihe:iti:2007:RetrieveDocumentSet</wsa:Action>
 </soapenv:Header>
 <soapenv:Body>
  <RetrieveDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="urn:ihe:iti:xds-b:2007
          file:/Users/bill/ihe/Frameworks/ITI-4/XDS.b/schema/IHE/XDS.b_DocumentRepository.xsd">

    <DocumentRequest>
     <RepositoryUniqueId>1.19.6.24.109.42.1.5</RepositoryUniqueId>
     <DocumentUniqueId>160.27.80.47.1.54</DocumentUniqueId>
    </DocumentRequest>

  </RetrieveDocumentSetRequest>
 </soapenv:Body>
</soapenv:Envelope>
--MIMEBoundaryurn_uuid_6C0A7AC4D92351F45B1268908711218--
```

要求するドキュメントの情報

図 B-22 リポジトリへの文書取得要求メッセージ

それに対して文書取得結果メッセージには、要求された文書本体が含まれる。

図 B-23 の文書取得結果メッセージにおいて、SOAP メッセージの Body 部に DocumentResponse タグがあるが、これは取得した文書の情報が記述される。文書本体は SOAP メッセージの添付データとして取り扱われる。DocumentResponse タグと文書本体は、DocumentResponse タグ内にある Document タグで対応付けられる。

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: multipart/related;
boundary=MIMEBoundaryurn_uuid_D93C36CAA0149E1BB01268908713305;
type="application/xop+xml";
start="0.urn:uuid:D93C36CAA0149E1BB01268908713306@apache.org";
start-info="application/soap+xml"; action="urn:ihe:iti:2007:RetrieveDocumentSetResponse"
Transfer-Encoding: chunked
Date: Thu, 18 Mar 2010 10:38:32 GMT

--MIMEBoundaryurn_uuid_D93C36CAA0149E1BB01268908713305
Content-Type: application/xop+xml; charset=UTF-8; type="application/soap+xml"
Content-Transfer-Encoding: binary
Content-ID: <0.urn:uuid:D93C36CAA0149E1BB01268908713306@apache.org>

<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
                  xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <soapenv:Header>
    <wsa:Action>urn:ihe:iti:2007:RetrieveDocumentSetResponse</wsa:Action>
    <wsa:RelatesTo>urn:uuid:6C0A7AC4D92351F45B1268908711215</wsa:RelatesTo>
  </soapenv:Header>
  <soapenv:Body>
    <xdsb:RetrieveDocumentSetResponse xmlns:xdsb="urn:ihe:iti:xds-b:2007">
      <rs:RegistryResponse xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
                           status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success" />

      <xdsb:DocumentResponse>
        <xdsb:RepositoryUniqueId>1.19.6.24.109.42.1.5</xdsb:RepositoryUniqueId>
        <xdsb:DocumentUniqueId>160.27.80.47.1.54</xdsb:DocumentUniqueId>
        <xdsb:mimeType>text/plain</xdsb:mimeType>
        <xdsb:Document>
          <xop:Include href="cid:1.urn:uuid:D93C36CAA0149E1BB01268908713308@apache.org"
                       xmlns:xop="http://www.w3.org/2004/08/xop/include" />
        </xdsb:Document>
      </xdsb:DocumentResponse>

    </xdsb:RetrieveDocumentSetResponse>
  </soapenv:Body>
</soapenv:Envelope>

--MIMEBoundaryurn_uuid_D93C36CAA0149E1BB01268908713305
Content-Type: text/plain
Content-Transfer-Encoding: binary
Content-ID: <1.urn:uuid:D93C36CAA0149E1BB01268908713308@apache.org>

This is my document.

It is great!

--MIMEBoundaryurn_uuid_D93C36CAA0149E1BB01268908713305--
```

取得したドキュメントの情報

取得したドキュメント本体

図 B-23 リポジトリからの文書取得結果

B.5　各アクタの設置形態

XDS に基づく地域医療連携システムを構築する場合には、定義されている各アクタをどのように配置するかが問題となる。各アクタの配置形態についてはさまざま考えられるが、ここでは例として以下のケースを取り上げる。

なお、XDS の各アクタがどのように配置されようとも、取り扱う患者情報は外部漏洩や不正利用などがないように安全に管理されなければならず、また安全に管理されるようシステム構築がなされなければならない。このため厚生労働省がいくつかのガイドラインを作成し、遵守を求めている。

・ケース 1（図 B-24）

ソース、リポジトリ、コンシューマは各医療機関にて維持管理し、レジストリは第三者機関に 1 つだけ設置して各医療機関からのメタデータを集中管理する。ここで第三者機関とは医療機関だけでなく、行政機関などが開設したデータセンター、ならびに医療機関などの委託をうけて情報を保管する民間のデータセンターをも指す。

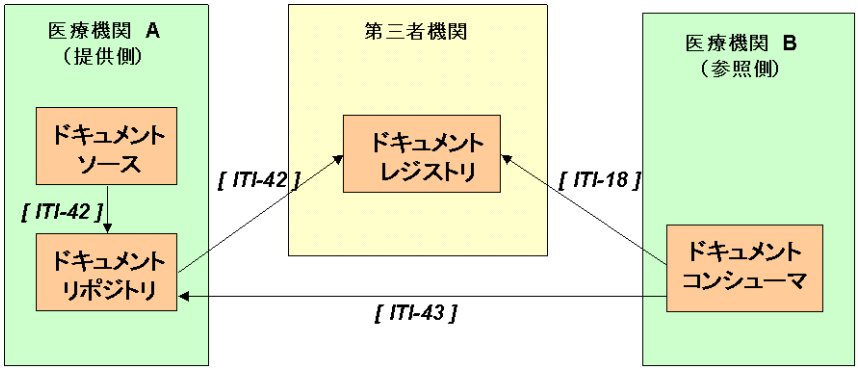


図 B-24　ケース 1

・ケース 2：(図 B-25)

ソース、コンシューマは各医療機関にて維持管理し、レジストリ、リポジトリは第三者機関にそれぞれ 1 つ設置し管理するもの。各医療機関からの文書本体及びメタデータはこの第三者機関において集中管理される。なお、ここで言う第三者機関はケース 1 と同じ。

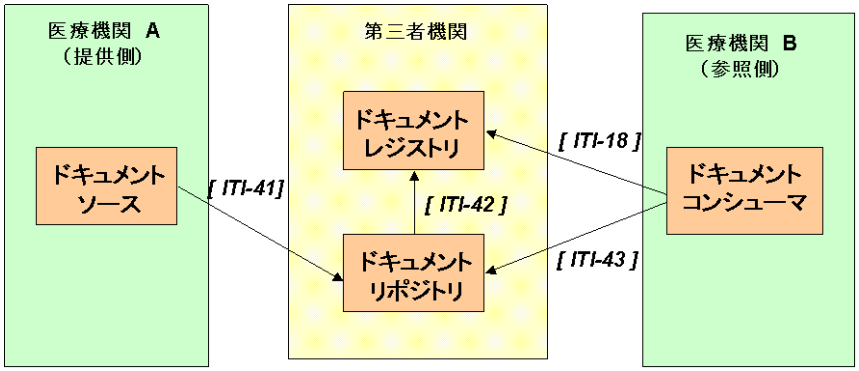


図 B-25 ケース2

B.6 各アクタが持つべき機能

B.6.1 ドキュメントソース

ドキュメントソース（ソース）が関連するトランザクションは表 B-15 の通りである。

表 B-15 ソースが関連するトランザクション

トランザクション	ソース/ターゲット
Provider And Register Document Set-b [ITI-41]	ソース

表 B-15 のトランザクションに対応するためにソースに実装する機能として、以下の機能（１）～（３）がある。このうち（１）は必須の機能である。

（１）文書の登録（必須）

１つ、あるいは複数の文書がソースからレジストリ、リポジトリへ登録できるようにする。そのためには以下の項目が必要となる

- 登録する文書の選択
- メタデータの作成
- インタフェース。リポジトリに対して、MTOM/XOP 形式の SOAP メッセージで文書とそのメタデータが送信でき、かつリポジトリからの返信メッセージが受信できるインタフェース。

（２）文書間関係の定義

B.3（５）で説明した文書の関連が定義できるようにする。これを実現するには以下の項目ができる機能が必要である。

- 新規文書を、既に登録済みの文書に対する差し替え(RPLC)、添付(APND)、変換（XFRM)、あるいは変換の上差し替え（XFRM_RPLC）として登録
- 既に登録済みの２つの文書に、差し替え(RPLC)、添付(APND)、変換(XFRM)、あるいは変換の上差し替え（XFRM_RPLC）という関係を定義する

・ 新規に登録する文書、あるいは既に登録済みの文書に電子署名を付与する。

ただし、既に登録済みの文書に対して文書間関係を定義する場合は、登録済み文書のメタデータ（ドキュメントエントリ）にレジストリが付与した entryUUID 値がソース側で必要となる。この entryUUID をレジストリから取得する場合、さらに

・ ドキュメントエントリの検索機能

が必要となるかもしれない。これはコンシューマにおいて実装されるメタデータの検索機能と同じものである。

（3）フォルダの管理

文書の管理・取りまとめるために、フォルダを登録、管理できるようにする。これを実現するには、

・ フォルダの新規登録（メタデータの作成を含む）
・ フォルダへの文書追加

ができる機能が必要である。

ただし、既に登録済みのフォルダに文書を追加する場合は、登録済みフォルダのメタデータにレジストリが付与した entryUUID 値がソース側で必要となる。この entryUUID をレジストリから取得する場合、さらに

・ フォルダの検索機能

が必要となるかもしれない。これはコンシューマにおいて実装されるメタデータの検索機能と同じものである。

B.6.2 ドキュメントリポジトリ

ドキュメントリポジトリ(リポジトリ)に関連するトランザクションは表 B-16 の通りである。

表 B-16 リポジトリに関連するトランザクション

トランザクション	ソース/ターゲット
Provider And Register Document Set-b [ITI-41]	ターゲット
Register Document Set-b [ITI-42]	ソース
Retrieve Document Set [ITI-43]	ターゲット

表 B-16 のトランザクションに対応するためにリポジトリに実装する機能として、以下の機能が必要である。

（1） 文書の保存

トランザクション［ITI-41］に従いドキュメントソースから送られてくる登録要求メッセージから、文書を取り出して保存する。これを実現するには、以

下の機能を実装する。

なお、登録要求メッセージにサブミッションセット、フォルダとアソシエーションだけ含まれている場合は以下の機能は実行しなくてもよい。

・インタフェース。

ソースからの MTOM/XOP 形式の SOAP メッセージが受信でき、かつソースに対して返信メッセージが送信できるインタフェースが必要。登録要求メッセージから文書本体を抽出

・ ドキュメントエントリの uniqueId の検証

リポジトリでは、抽出文書とそのドキュメントエントリに含まれる uniqueId 値とを対応付けて保存する。そのため、uniqueId が本当にユニークであるかを検証する必要がある。

・ サブミッションセットの sourceId の検証

ソースからのアクセスを制限している場合は、登録要求メッセージがアクセスを許可したソースからのものかを検証する必要がある。その場合、sourceId 値はソース固有の ID が設定されているので、これをチェックする。

・ 抽出文書の保存

抽出文書とそのドキュメントエントリに含まれるuniqueId値とを対応付けて保存する。文書の保存には、ファイルとして保存する場合、データベースツールを利用する場合などがある。なお、文書のハッシュ値及びサイズを計算しておく。これらは次の（２）で使用する。

（２） メタデータの登録

上記（１）で文書抽出後、トランザクション[ITI-42]に従い、登録要求メッセージに含まれるメタデータをレジストリへ送る。これを実行するために以下の機能が必要となる。

・ 文書情報をメタデータへ追加

リポジトリに保存する文書に関係する情報を、保存文書のドキュメントエントリの属性値として追加する。追加対象となる属性は表 C－１７の通り。なおリポジトリそのものを表す固有 ID をあらかじめ決めておかなければならない。

表 B-17 追加対象となる属性

ドキュメントエントリの属性値	必要性	設定値
hash	R	文書のハッシュ値
size	R	文書をファイル化した時のサイズ
RepositoryUniqueId	R	文書を保存するリポジトリに割り当てられた固有のID
URI	O	文書へアクセス可能なURI

凡例 R:必須 O:任意

・ インタフェース

レジストリに対して、SOAP メッセージでメタデータが送信でき、かつレジストリからの返信メッセージが受信できるインタフェースが必要。

（3）文書取得要求に対する対応

トランザクション[ITI-43]に従い、コンシューマからの文書取得要求メッセージを受け取ると、リポジトリはその要求に応じた文書をコンシューマへ送る。機能としては以下が必要となる。

・ インタフェース

コンシューマからの文書取得要求メッセージが取得でき、コンシューマへ要求に応じた文書を送ることができる。送受信メッセージとして MTOM/XOP 形式の SOAP メッセージを取り扱えるようにするのが必須だが、オプションとして URI による HTTP 形式の利用も認められている(ただし、トランザクションは[ITI-43]とは別のトランザクション[ITI-17]となる)。

・ 要求に応じた文書を用意する

トランザクション[ITI-43]に従う場合、文書取得要求メッセージには、取得したい文書の情報として、文書のドキュメントエントリの属性である uniqueId が含まれている。リポジトリは uniqueId に合致する文書を取り出し、コンシューマへ送る準備をする。

またトランザクション[ITI-17]に従う場合は、コンシューマから URI を通じたアクセスがあった場合は､HTTP GET を利用して文書を送信する。ただしこの場合、あらかじめ文書は URI によるアクセスができる場所においておく必要がある。

（4）エラー処理

リポジトリにおいてエラーが発生した場合は、呼び出し元（ソース、コンシューマ）にエラーメッセージを送る。XDS ではどの場合にどのようなエラーを発生させるかが決まっている。エラーについての詳細は IHE-TF-3 の 4.1.13 を参照のこと。

トランザクション[ITI-41][ITI-42]におけるドキュメント登録において、レジストリ側でエラーが発生した場合はエラーメッセージをレジストリから受け取る。このとき、リポジトリでは保存したドキュメント本体を削除したうえで、ソースへエラーメッセージを送る。

B.6.3 ドキュメントレジストリ

ドキュメントレジストリ(レジストリ)に関連するトランザクションは表 B-18 の通りである。

表 B-18 レジストリに関連するトランザクション

トランザクション	ソース/ターゲット
Register Document Set-b [ITI-42]	ターゲット
Registry Stored Query [ITI-18]	ターゲット
Patient Identity Feed [ITI-8] *	ターゲット
Patient Identity Feed HL7v3 [ITI-44] *	ターゲット

注:本節では*印のトランザクションにかかわる処理については記述しない

表 B-18 のトランザクションに対応するためにレジストリに実装する機能として、以下の機能が必要である。ただし本節では、Patient Identity Feed に関する[ITI-8]及び[ITI-44]に対する機能は触れない。

（1）メタデータの登録

トランザクション[ITI-42]に従い、レジストリが登録要求メッセージを受け取ると、これに含まれるメタデータをレジストリに保存する。メタデータは形式、内容が検証され、XDS で定義された形式に従っていると判断されたものが保存される。これを実行するために以下の機能が必要となる。

・インタフェース

リポジトリからの登録要求メッセージを含む SOAP メッセージが受け取れるようにする。またリポジトリへの返信メッセージが送れるようにする。

・メタデータの検証

登録要求メッセージに含まれるメタデータの形式が IHE-TF-3 の 4.1.7(ドキュメントエントリ)、4.1.8（サブミッションセット)、及び 4.1.9（フォルダ）で定義された形式と合致していることを確認する。

またメタデータの各属性値には、IHE-TF-3 の 4.1.10 で定義されているような制約があるので、各属性値が制約を満たしていることを確認する。

・メタデータの属性追加

レジストリ側でメタデータの属性を新規追加する。新規追加の対象となる属性を表 B-19 に示す。

表 B-19 追加対象となる属性

メタデータの種類	属性	備考
ドキュメントエントリ	availabilityStatus	新規登録時に「urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Approved」とする。
	entryUUID	UUID値で指定する。UUIDの形式はIHE-TF-3の4.1.7にあるTable4.1-3を参照
	homeCommunityId	オプションだが、XCAを利用して複数コミュニティを連携させる場合は必須
フォルダ	availabilityStatus	新規登録時に「urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Approved」とする。
	entryUUID	UUID値で指定する。UUIDの形式はIHE-TF-3の4.1.7にあるTable4.1-3を参照
	homeCommunityId	オプションだが、XCAを利用して複数コミュニティを連携させる場合は必須
	lastUadateTime	新規に登録された時の時間
サブミッションセット	availabilityStatus	新規登録時に「urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Approved」とする。
	entryUUID	UUID値で指定する。UUIDの形式はIHE-TF-3の4.1.7にあるTable4.1-3を参照
	homeCommunityId	オプションだが、XCAを利用して複数コミュニティを連携させる場合は必須

- 患者 ID の検証
  ドキュメントエントリに含まれる患者 ID が、該当のコミュニティにおいて有効かどうかを調べる。
- 登録データのアトミック性の保障
  登録要求メッセージに含まれるすべてのメタデータが無事登録できた場合は、登録成功（Success）の返信メッセージをリポジトリへ送る。
  しかし、登録要求メッセージに含まれるメタデータのうち、エラー発生などで一つでも登録に失敗した場合は、その登録要求メッセージに含まれるメタデータで登録に成功したものをすべて削除し、エラーメッセージをリポジトリへ送る。エラーについては後述のエラー処理を参照のこと。すなわち、この場合は登録要求そのものをなかったものとすることになる。
- 文書の置き換え
  登録要求メッセージに文書の置き換え（RPLC、XFRM_RPLC）を含む場合は、置き換えられる文書のドキュメントエントリが登録済みであること、その availabilityStatus が Approved であることを確認した上で、置き換えられるドキュメントエントリの availabilityStatus を Duplicated に変更する。
- フォルダの患者 ID の検証
  フォルダのメタデータ属性である patientId の値とフォルダに属するドキュメントエントリのメタデータ属性 patientId の値が一致すること

を確認する。

- MIME タイプの検証
  ドキュメントエントリのメタデータ属性 mimeType で指定されている MIME タイプが XDS アフィニティドメインで指定されているものであるかを調べる。
- フォルダの属性 lastUpdateTime の維持管理
  既に登録されているフォルダに新規にドキュメントエントリを追加した場合、フォルダのメタデータ属性 lastUpdateTime が追加した時間に再設定する。
- フォルダに追加する文書の患者 ID の検証
  既に登録されているフォルダに新規にドキュメントエントリを追加する場合、フォルダの patientId とドキュメントエントリの patientId が一致することを確認する。
- コード数の確認
  メタデータ属性の中には、複数設定できるものもあれば（例：ドキュメントエントリの author、eventCodeList など)、一つのみ設定できるもの（例：ドキュメントエントリの classCode）もある。属性が適切な数量だけ設定できているかどうかを調べる。
- メタデータの保存
  登録要求メッセージに含まれるメタデータを適正に保存する。登録要求メッセージに複数のドキュメントエントリが含まれていても同様である。

（2）検索要求に対する対応

トランザクション[ITI-18]に従って、コンシューマ (場合によってはソース) からの検索要求メッセージを受け取ると、レジストリはそのメッセージで指定されているストアドクエリに従い、レジストリが保存しているメタデータの中から、検索要求メッセージに含まれる検索条件に沿ったメタデータを捜す。

ストアドクエリの種類は表　にしめす。なおストアドクエリの種類ごとにコンシューマで設定可能な検索条件が決まっている。詳細な説明は ITI-TF-2a の 3.18.4.1.2.3.6.1 を参照のこと。

（3）エラー処理

レジストリにおいてエラーが発生した場合は、呼び出し元にエラーメッセージを送る。

XDS ではどの場合にどのようなエラーを発生させるかが決まっている。エラーについての詳細は ITI-TF-3 の 4.1.13 を参照のこと。

上記（1）で述べたようにトランザクション[ITI-42]の実行過程で発生した場合は、登録要求そのものをなかったものとする必要があるため、以下の処理を行う。

- 登録要求メッセージに含まれるメタデータで登録に成功したものをすべて削除する。

・ lastUpdateTime を更新していた場合は元の時間に戻す。
・ 文書置き換え処理を実行した場合は、Duplicated に置き換えられたドキュメントエントリの availabilityStatus を元の Approved に戻す。

B.6.4 ドキュメントコンシューマ

ドキュメントコンシューマ（コンシューマ）に関連するトランザクションは表 B-20 の通りである。

表 B-20 コンシューマに関連するトランザクション

トランザクション	ソース/ターゲット
Registry Stored Query [ITI-18]	ソース
Retrieve Document Set [ITI-43]	ソース

表 B-20 のトランザクションに対応するためにレジストリに実装する機能として、以下の機能が必要である。

（1）メタデータ検索

メタデータ検索はトランザクション[ITI-18]に従い、ストアドクエリにより行う。レジストリがどのストアドクエリをサポートしているかを調べた上で、以下の機能を実装する。なお、以下の機能はいずれも GUI を利用してメッセージ作成や結果の提示を行うことになる。

・ 検索要求メッセージ作成
　ストアドクエリと検索条件を設定し、これをレジストリへ送る。なおストアドクエリの種類ごとに設定可能な検索条件が決まっている。詳細な説明は ITI-TF-2a の 3.18.4.1.2.3.6.1 を参照のこと。
・ 検索結果提示
　レジストリからの返信メッセージから検索結果として含まれるメタデータを取り出し、利用者に提示する。検索結果の概要を一覧表で示す一覧表示、及び一つのメタデータの詳細を表示する詳細表示の 2 種類が考えられる。
・ インタフェース
　レジストリのと間で SOAP メッセージの送受信ができるようにする。

（2）文書取得

トランザクション[ITI-43]（または[ITI-17]）に従い、文書本体を取得する。そのために以下の機能が必要となる。

・ 文書取得要求メッセージ作成
　文書取得要求メッセージを作成し、これをリポジトリへ送る。文書取得要求メッセージは取得したい文書のドキュメントエントリに含まれる属性 uniqueId、mimeType 及び repositoryUniqueId で構成される。

- 取得文書の提示
  文書取得要求により、リポジトリから得られた文書を利用者に提示する。
- インタフェース
  リポジトリへの文書取得要求メッセージを MTOM/XOP 形式の SOAP メッセージで送信できるようにする。またリポジトリから文書が MTOM/XOP 形式の SOAP メッセージで送られてくるので、これを取り扱えるようにする。
  また URI を用いた文書取得を実行する場合には、HTTP GET での文書取得ができるようにする。

附属書 C.　ATNA, CT など

本附属書では、システム構築時に必要となるセキュリティ基盤について技術的な観点でまとめる。なお、セキュリティ環境の構築時のポリシーや考え方については４章「ネットワーク基盤」を参照されたい。また、具体的な監査証跡ログの形式については、附属書 D に記載する。

C.1　セキュリティ基盤概要

地域連携システム構築にあたり、構築するシステムのセキュリティポリシーに基づいて、どのようなメカニズムを利用してセキュリティを実現するか検討する必要がある。IHE にはこのような検討点を解決するために、IT インフラストラクチャ分野で、いくつかの業務シナリオを提供している。

ここでは、監査証跡ログについて記載されている ATNA(Audit Trail and Node Authentication)、文書・画像・監査証跡ログ等の情報を正しく集めるために時刻を一致させておくことができる CT(Consistent Time)を紹介する。

IHE の ITI 領域では、この他に、登録した文書や画像に対するアクセスコントロールを実現している BPPC(Basic Patient Privacy Consents)、利用者認証に活用できる　EUA(Enterprise User Authentication), XUA(Cross-Enterprise User Assertion)などの統合プロファイルも提案されている。業務分析を行い、業務シナリオに合致した統合プロファイルがあれば利用することをお勧めする。

C.2　統合プロファイル各論

C.2.1　ATNA

(1)　統合プロファイル概要

① 位置づけと背景

ATNA 統合プロファイルは IHE IT Infrastructure 領域の１つとして登録されており、2010 年 2 月現在の最新バージョンは、Revision 6.0（2008 年 8 月 10 日版）である。

② プロファイル概要

ATNA 統合プロファイルは、次の４つの項目の実現を目的とする。

1) ユーザへの説明責任（監査証跡）：組織のセキュリティ管理者による監査に基づく、安全性に関する領域内のポリシーの遵守の評価、保護すべき PHI(健康情報）に対する不適切な生成、アクセス、修正、削除の発見、

2) アクセス制御：ネットワークアクセスをノード間に制限し、各ノードに対して認可されたユーザにアクセスを制限する方法でのアクセス制御、

3) 集中監査記録リポジトリ：全ての IHE アクタから、監査証跡リポジトリへの監査記録の転送が必要、

4) PHI（Protected Health Information）の完全性：PHI の有効期間とその過程におけるデータの完全性の追跡。

ATNA 統合プロファイルは、次のような条件を元に検討されている。
1)“Secure Domain”に参加しているシステムは、ATNA プロファイルのセキュリティノードアクタとトランザクションを実装している。
2) セキュアノード上の全てのアプリケーションはこれらが IHE アクタであるか否かにかかわらず ATNA の要求に従う。
3) ATNA 統合プロファイルは、ネットワーク攻撃やウィルス汚染などの、他のセキュリティ要求については言及しない。
4) IHE は転送時の暗号の使用は要求しない。他の認可されたセキュアノードと通信する手段として TLS セキュリティネゴシエーションの仕組みを要求する。
5) ATNA はローカルなユーザ認証のみを要求する。EUA も選択の一つだが、これを使う必要は無い。
6) 携帯機器に関する特別な面には言及しない。

接続認証(Node Authentication)については、次の要件が記載されている。
1) 各ノードの接続に対して、双方向の証明書ベースのノード認証を要求する。
2) DICOM,HL7,HTML の各プロトコルは全て証明書ベースの決まった認証機構を持っている。ユーザではなく、ノードを認証している。
3) 双方向のノード認証ができない機器の接続は禁止されるか、PHI アクセスを防ぐようにする。

監査証跡(Audit Trail)については、次の要件が記載されている。
1) 監査は常に選択したアクセス制御と認証方法とは独立していなければならない。
2) 記録は単に個々の IHE アクタに相当する個々のコンポーネントだけではなく、全体のプロセスに対するイベントの記述を捕まえなければならない。
3) 監査記録メッセージは、集中監査リポジトリへログ採取が行われる。仕組みは、Reliable Syslog Cooked Profile(RFC-3195)に使い方を規定している。BSD Syslog(RFC-3164)も使用可能だが制約がある。

①参照する標準規格
ATNA ではトランザクションにより異なる標準規格を参照している。
１）トランザクション「時間保守機能」
NTP Network Time Protocol Version 3. RFC1305
SNTP Simple Network Time Protocol (SNTP) RFC2030

２）トランザクション「ノード認証」
DICOM 2003 PS 3.15:Security Profiles. Annex B1:The Basic TLS Secure Transport Connection profile
IETF: Transport Layer Security (TLS) 1.0 (RFC 2246)
ITU-T: Recommendation X.509 (03/00). “Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks”

３）トランザクション「監査イベント記録」

IETF: The BSD Syslog Protocol. (RFC 3164);Reliable Delivery for Syslog (RFC 3195);Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications (RFC 3881).

DICOM Supplement 95, c)ASTM: E2147-01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems.

W3C: Recommendation: Extensible Markup Language (XML) 1.0

②監査イベント記録

ATNA では取得するべき監査イベント記録が規定されている。DICOM 等で定義されているものの他に IHE 独自に定義しているイベントが多数ある。また、イベントは CP 等で都度追加／訂正されているのが実情である。

（２）利用方法

ATNA 統合プロファイルは、ノード認証・監査証跡（時間保守含む）共に導入についての技術的な問題点は存在しないと考える。今後、益々ログ情報等の取得が医療情報システムの運用時の重要な要件となることは間違いないので導入を進めるべき分野だといえる。

ATNA 統合プロファイルを医療機関内で利用する場合は、許可されないシステムや機器が導入されている可能性が低いので NA(Node Authentication)は導入の必要性は低いと考える。地域医療連携システムについてもどのようなネットワーク環境を利用して施設同士を接続するかにより、NA の導入要否を検討すればよいだろう。

AT(Audit Trail)機能については、施設内のシステムや利用状況の監査よりもより厳密に監査し導入すべきである。但し、監査証跡で取得すべきイベントについては、その要否及び過不足について十分な検討が必要である。

C.2.2 CT

（１）統合プロファイル概要

CT は、対象となるシステムを構成する各装置の内部時計の時刻を合わせる機能を提供する。これにより、データの生成時刻などの整合性を保つとともに、取り扱う情報のセキュリティを担保するための監査証跡の有効性を高めることができる。本プロファイルでは、基準となる時計を持つ Time Server との通信により、各装置の内部時計を合わせるトランザクションが規定されている。

（２）利用方法

CT 統合プロファイルによる時刻同期は、正確な監査証跡の取得や障害発生時の切り分け情報のために大切な機能である。利用には、まず施設内にタイムサーバを導入することが必須である。現在では、電波で正確な時刻を取得してタイムサーバ機能を実現する機器も販売されているので活用いただきたい。さら

に、クライアント PC の OS に標準に実現されている時刻合わせ機能での設定でよいので、時刻同期を行いシステム内のサーバ・クライアントがすべて同じ時刻となるように運用することを推奨する。

C.3　監査証跡の要求仕様書記載のポイント

（ポイント１）

実現するシステムの各機能で、

a)ノード認証、

b)監査証跡ログの出力、

c)時刻同期

の実施を行う旨を記載する。

特に、いつどのようなタイミングで認証、ログ出力を実施するか、また、時刻同期を行う頻度などは明確にする必要がある。特に監査証跡ログを出力するイベントは十分検討する必要がある。

（ポイント２）

ノード認証、監査証跡ログ機能、時刻同期の基本的な手順及び技術的なメカニズムについては別途まとめるとよい。

C.3.1　監査証跡ログを記載するイベントの抽出方法

監査証跡ログを記載すべきイベントについては、テクニカルフレームワークに記載されている情報を参考に、各システムで検討する必要がある。また、IT インフラストラクチャのテクニカルフレームワークには、統合プロファイルごとに出力する監査証跡ログの記載がある。こちらもあわせて確認する必要がある。

ITI のテクニカフレームワークが参照しているログイベントは、DICOM 規格の Supplement95”Audit Trail Messages”である。あわせて確認願いたい。

表 C-1　監査証跡ログ出力のトリガーイベント一覧

Trigger Event	Description	Source Vocabulary
Instances-Stored	Instances for a particular study have been stored on this system. One event covers all instances stored for the particular study.	DICOM (Sup 95) “DICOM Instances Transferred”
Medication	Medication orders and administration within an instance or episode of care. This includes initial order, dispensing, delivery, and cancellation. See note below.	IHE Extension (ITI TF-2a: 3.20.7.3) “Medication Event”
Mobile-machine-event	Mobile machine joins or leaves secure domain.	DICOM (Sup 95) “Network Entry”
Node-Authentication-failure	A secure node authentication failure has occurred during TLS negotiation, e.g. invalid certificate.	DICOM (Sup 95) “Security Alert”
Order-record-event	Order record created, accessed, modified or deleted. Involved actors: Order Placer. This includes initial order, updates or amendments, delivery, completion, and cancellation. See note below.	DICOM (Sup 95) “Order Record”
Patient-care-assignment	Staffing or participant assignment actions relevant to	IHE Extension (ITI TF-2a:

	the assignment of healthcare professionals, caregivers attending physician, residents, medical students, consultants, etc. to a patient It also includes change in assigned role or authorization, e.g., relative to healthcare status change, and de-assignment	3.20.7.3) “Patient Care Resource Assignment”
Patient-care-protocol	Patient association with a care protocol. This includes initial assignment, scheduling, updates or amendments, completion, and cancellation. See note below.	IHE Extension (ITI TF-2a: 3.20.7.3) “Patient Care Protocol”
Patient-record-event	Patient record created, modified, or accessed.	DICOM (Sup 95) “Patient Record”
PHI-export	Any export of PHI on media, either removable physical media such as CD-ROM or electronic transfer of files such as email. Any printing activity, paper or film, local or remote, that prints PHI.	DICOM (Sup 95) “Export”
PHI-import	Any import of PHI on media, either removable physical media such as CD-ROM or electronic transfers of files such as email.	DICOM (Sup 95) “Import”
Procedure-record-event	Procedure record created, modified, accessed or deleted.	DICOM (Sup 95) “Procedure Record”
Query Information	A query has been received, either as part of an IHE transaction, or as part other products functions. For example: 1) Modality Worklist Query 2) Instance or Image Availability Query 3) PIX, PDQ, or XDS Query Notes: The general guideance is to log the query event with the query parameters and not the result of the query. The result of a query may be very large and is likely to be of limited value vs the overhead. The query parameters can be used effectively to detect bad behavor and the expectation is that given the query parameters the result could be See note below.	DICOM (Sup 95) “Query”
Mobile-machine-event	Mobile machine joins or leaves secure domain.	DICOM (Sup 95) “Network Entry”
Node-Authentication-failure	A secure node authentication failure has occurred during TLS negotiation, e.g. invalid certificate.	DICOM (Sup 95) “Security Alert”
Order-record-event	Order record created, accessed, modified or deleted. Involved actors: Order Placer. This includes initial order, updates or amendments, delivery, completion, and cancellation. See note below.	DICOM (Sup 95) “Order Record”
Patient-care-assignment	Staffing or participant assignment actions relevant to the assignment of healthcare professionals, caregivers attending physician, residents, medical students, consultants, etc. to a patient It also includes change in assigned role or authorization, e.g., relative to healthcare status change, and de-assignment	IHE Extension (ITI TF-2a: 3.20.7.3) “Patient Care Resource Assignment”
Patient-care-episode	Specific patient care episodes or problems that occur within an instance of care. This includes initial assignment, updates or amendments, resolution, completion, and cancellation. See note below.	IHE Extension (ITI TF-2a: 3.20.7.3) “Patient Care Episode”
Patient-care-protocol	Patient association with a care protocol. This includes initial assignment, scheduling, updates or amendments, completion, and cancellation. See note below.	IHE Extension (ITI TF-2a: 3.20.7.3) “Patient Care Protocol”
Patient-record-event	Patient record created, modified, or accessed.	DICOM (Sup 95) “Patient Record”
PHI-export	Any export of PHI on media, either removable physical media such as CD-ROM or electronic transfer of files such as email. Any printing activity, paper or film, local or remote, that prints PHI.	DICOM (Sup 95) “Export”

PHI-import	Any import of PHI on media, either removable physical media such as CD-ROM or electronic transfers of files such as email.	DICOM (Sup 95) “Import”
Procedure-record-event	Procedure record created, modified, accessed or deleted.	DICOM (Sup 95) “Procedure Record”
Query Information	A query has been received, either as part of an IHE transaction, or as part other products functions. For example: 1) Modality Worklist Query 2) Instance or Image Availability Query 3) PIX, PDQ, or XDS Query Notes: The general guideance is to log the query event with the query parameters and not the result of the query. The result of a query may be very large and is likely to be of limited value vs the overhead. The query parameters can be used effectively to detect bad behavor and the expectation is that given the query parameters the result could be regenerated if necessary.	DICOM (Sup 95) “Query”
Security Alert	Security Administrative actions create, modify, delete, query, and display the following: 1. Configuration and other changes, e.g., software updates that affect any software that processes protected information. Hardware changes may also be reported in this event. 2. Security attributes and auditable events for the application functions used for patient management, clinical processes, registry of business objects and methods (e.g. WSDL, UDDI), program creation and maintenance, etc. 3. Security domains according to various organizational categories such as entity-wide, institutional, departmental, etc. 4. Security categories or groupings for functions and data such as patient management, nursing, clinical, etc. 5. The allowable access permissions associated with functions and data, such as create, read, update, delete, and execution of specific functional units or object access or manipulation methods. 6. Security roles according to various task-grouping categories such as security administration, admissions desk, nurses, physicians, clinical specialists, etc. It also includes the association of permissions with roles for role-based access control. 7. User accounts. This includes assigning or changing password or other authentication data. It also includes the association of roles with users for role-based access control, or permissions with users for user-based access control. 8. Unauthorized user attempt to use security administration functions. 9. Audit enabling and disabling. 10. User authentication revocation. 11. Emergency Mode Access (aka Break-Glass) Security administration events should always be audited.	DICOM (Sup 95) “Security Alert”
User Authentication	This message describes the event of a user attempting to log on or log off, whether successful or not. No Participant Objects are needed for this message.	DICOM (Sup 95) “User Authentication”
Study-Object-Event	Study is created, modified, accessed, or deleted. This reports on addition of new instances to existing studies as well as creation of new studies.	DICOM (Sup 95) “DICOM Instances Accessed”

Study-used	SOP Instances from a specific study are created, modified or accessed. One event covers all instances used for the particular study.	DICOM (Sup 95) “DICOM Instances Accessed”

Note: The IHE extension has reduced the scope of many of the IETF events to remove phrases like ―checking for clinical contra-indications‖. This is done to highlight that the events should be reported are those that are related to the access, use,

表 C-2 監査証跡ログ出力イベントのコード値一覧

Coding Scheme Designator	Coding Scheme Version	Code Value	Code Meaning
IHE		IHE0001	Health Services Provision Event
IHE		IHE0002	Medication Event
IHE		IHE0003	Patient Care ResourceAssignment
IHE		IHE0004	Patient Care Episode
IHE		IHE0005	Patient Care Protocol

補足:表 C-1 は、DICOM 規格から抜粋したトリガーイベントである。表 C-2 は、IHE が独自に検討して定義した監査証跡ログ出力イベントのコード値である。

C.3.2 監査証跡ログイベントの例

トリガーイベントを参考に監査証跡ログを出力すべきイベントをいくつか挙げる。実際には、実現するシステムに適したイベントを検討する必要があるので留意されたい。

＜イベント例＞

1) システムの起動／終了
2) ログサーバの起動／終了
3) ユーザ認証実行
4) ユーザ認証失敗（セキュリティアラート）
5) 文書／画像データ登録
6) 文書／画像データ検索
7) 文書／画像データ参照
8) 文書／画像データ抽出 export
9) 患者データの検索

C.3.3 監査証跡ログに記載すべきこと

監査メッセージの書式として RFC3881 で定義されたものを使用する。

監査メッセージには、「誰が」、「いつ」、「どのサーバ／端末から」、「どのサーバ／端末へ」、「どのデータに対して」「どうしたか」が記述される。本資料作成時には RFC2881 に定義されている監査証跡ログのスキーマ（メッセージ構造）はリタイアされていて取得することができない。附属書 D.3 に当該スキーマを

掲載する。

C.4　監査ログ関連の仕様書記載例

文書情報登録機能について、１）監査証跡ログ出力、2)時刻同期を実現するための記載例を以下に示す。

文書情報登録機能は、以下の要件を満たすこと。

① 作成された pdf 形式のデータファイルを地域連携サーバに登録する機能を有することと。

② 地域連携サーバに登録時には登録した旨を示す監査証跡ログを出力すること。監査証跡ログの出力は、IHE-IT インフラストラクチャ領域の ATNA(Audit Trail and Node Authentication)統合プロファイルの Audit Trail-Secure Node アクタを利用すること。

③ 監査証跡ログのイベント ID 等ログ内容の詳細は別途指定したとおりとすること。

④ 正確な情報収集のために、時刻サーバを導入する予定である。文書登録機能は、指定した時刻サーバと時刻同期を行うこと。時刻同期には、ITI-IT インフラストラクチャの CT(Consistent Time)統合プロファイルの Time Client アクタを利用すること。時刻同期は１回／日で実施することとする。実施時間は別途調整する。

附属書 D.　ATNA ログの例

本附属書では、具体的な監査証跡ログの形式について提示する。

D.1　監査証跡ログのユースケース

① 患者 A は、心臓が悪い。
② 自宅で、息切れと疲労感を自覚し、地域連携システムの機能を利用し、自分の医療情報を外部に持ち出す準備を行う。
③ かかりつけ医は、EMR へ患者 A の医療情報を取り込む。診察の結果、循環器科への受診を決め、紹介状を作成し、地域連携システムへ登録する。
④ 循環器医は、かかりつけ医からの紹介状を見て個人記録へ追加する。患者 A は診察時に胸部痛を訴えたため、救急外来に紹介する。
⑤ 患者 A の隣に住んでいる医師 BB は同じ循環器科で働いており、患者 A が受診したことに気づく。医師 BB は、自身の ID で患者 A の記録を入手しようとするが責任者でないため、不可となる。
⑥ 救急外来では、循環器医からの紹介状を参照する。救急外来医は特権を必要としないので、患者 A の記録を参照することが可能である。
⑦ プライバシ部門責任者は、患者 A の監査証跡ログから異常な事象の警告を得る。報告内容は、医師 BB の不正な医療情報入手の企てや、救急外来医による救急目的の医療情報参照を表示する。この報告は、開示用ログの作成にも役立つ。

D.2 監査証跡ログの出力形式

（１）文書データ取得時に、文書データを取得する側（Consumer）が出力

	Field Name	Opt	Value Constraints
Event AuditMessage/ EventIdentification	EventID	M	EV(110107, DCM, "Import")
	EventActionCode	M	"C" (Create)
	EventDataTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	EV("ITI-17", "IHE Transactions", "Retrieve Document")
Source (Document Repository) (1)			
Destination (Document Consumer) (1)			
Human Requestor (0..n)			
Audit Source (1)			
Patient (0..1)			
Document URI (1)			

Where:

	Field Name	Opt	Value Constraints
Source AuditMessage/ ActiveParticipant	UserID	U	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP adress
	NetworkAccessPointID	M	The machine name or IP adress, as specified in RFC 3881.
	Field Name	**Opt**	**Value Constraints**
Destination AuditMessage/ ActiveParitcipant	UserID	U	not specialized
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	U	not specialized
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP adress
	NetworkAccessPointID	M	The machine name or IP adress, as specified in RFC 3881.
Human Requestor (if known)	**Field Name**	**Opt**	Value Constraints
	U serID	M	Identity of the human that initiated the transaction.

AuditMessage/ ActiveParticipant	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	
Audit Source AuditMessage/ AuditSource Identification	**Field Name**	**Opt**	Value Constraints
	AuditSourceID	U	not specialized
	AuditEnterpriseSiteID	U	not specialized
	AuditSourceTypeCode	U	not specialized
Patient (if known) AuditMessage/ ParticipantObjectIdentification	**Field Name**	**Opt**	Value Constraints
	ParticipantObjectTypeCode	M	"1" (Person)
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
Document URI AuditMessage/ ParticipantObjectIdentification	**Field Name**	**Opt**	**Value Constraints**
	ParticipantObjectTypeCode	M	"2" (system)
	ParticipantObjectTypeCodeRole	M	"3" (report)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV(12, RFC-3881, "URI")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	Document URI
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	MC	Type=XDSDocumentEntry.uniqueId (the literal string), Value=the value of the Document Unique ID (from the XDS metadata)

（2）文書データ取得時に、文書データを提供する側（Repository）が出力

Event AuditMessage/ EventIdentification	**Field Name**	**Opt**	**Value Constraints**
	EventID	M	EV(110107, DCM, "Import")
	EventActionCode	M	"C" (Create)
	EventDataTime	M	not specialized

	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	EV("ITI-17", "IHE Transactions", "Retrieve Document")
Source (Document Repository) (1)			
Destination (Document Consumer) (1)			
Human Requestor (0..n)			
Audit Source (1)			
Patient (0..1)			
Document URI (1)			

Where:

	Field Name	Opt	Value Constraints
Source AuditMessage/ ActiveParticipant	UserID	U	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP adress
	NetworkAccessPointID	M	The machine name or IP adress, as specified in RFC 3881.
Destination AuditMessage/ ActiveParticipant	**Field Name**	**Opt**	**Value Constraints**
	UserID	U	not specialized
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	U	not specialized
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP adress
	NetworkAccessPointID	M	The machine name or IP adress, as specified in RFC 3881.
Human Requestor (if known) AuditMessage/ ActiveParticipant	**Field Name**	**Opt**	**Value Constraints**
	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	
Audit Source AuditMessage/	**Field Name**	**Opt**	**Value Constraints**
	AuditSourceID	U	not specialized

AuditSource Identification	AuditEnterpriseSiteID	U	not specialized
	AuditSourceTypeCode	U	not specialized
Patient (if known) AuditMessage/ ParticipantObjectIdentification	**Field Name**	**Opt**	**Value Constraints**
	ParticipantObjectTypeCode	M	"1" (Person)
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID in HL7 CX format.
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
Document URI AuditMessage/ ParticipantObjectIdentification	**Field Name**	**Opt**	**Value Constraints**
	ParticipantObjectTypeCode	M	"2" (system)
	ParticipantObjectTypeCodeRole	M	"3" (report)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV(12, RFC-3881, "URI")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	Document URI
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	MC	Type=XDSDocumentEntry.uniqueId (the literal string), Value=the value of the Document Unique ID (from the XDS metadata)

（３）文書データ登録時に、文書を登録する側（Source）が出力

Event AuditMessage/ EventIdentification	**Field Name**	**Opt**	**Value Constraints**
	EventID	M	EV(110106, DCM, "Export")
	EventActionCode	M	"R" (Read)
	EventDataTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	EV("ITI-14", "IHE Transactions", "Register Document Set")
Source (Document Repository or Integrated Document Source/Repository) (1)			
Human Requestor (0..n)			
Destination (Document Registory) (1)			
Audit Source (Document Repository or Integrated Document Source/Repository) (1)			
Patient (1)			
SubmissionSet (1)			

Where:

Source	Field Name	Opt	Value Constraints

AuditMessage/ ActiveParticipant	UserID	U	not specialized
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	U	not specialized
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP adress
	NetworkAccessPointID	M	The machine name or IP adress, as specified in RFC 3881.
Human Requestor (if known) AuditMessage/ ActiveParticipant	**Field Name**	**Opt**	**Value Constraints**
	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"true"
	RoleIDCode	U	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	
Destination AuditMessage/ ActiveParticipant	**Field Name**	**Opt**	**Value Constraints**
	UserID	M	SOAP endpoint URI.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP adress
	NetworkAccessPointID	M	The machine name or IP adress, as specified in RFC 3881.
Audit Source AuditMessage/ AuditSource Identification	**Field Name**	**Opt**	**Value Constraints**
	AuditSourceID	U	not specialized
	AuditEnterpriseSiteID	U	not specialized
	AuditSourceTypeCode	U	not specialized
Patient AuditMessage/ ParticipantObject Identification	**Field Name**	**Opt**	**Value Constraints**
	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881,

			"Patient Number")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	the patient ID in HL7 CX format..
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
SubmissionSet AuditMessage/ ParticipantObject Identification	**Field Name**	**Opt**	**Value Constraints**
	ParticipantObjectTypeCode	M	"2" (System)
	ParticipantObjectTypeCodeRole	M	"20" (job)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV("urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd", "IHE XDS Metadata", "submission set classificationNode")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	the submissionSet unique ID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized

（4）文書データ登録時に、文書データを登録される側（Repository）が出力

	Field Name	**Opt**	**Value Constraints**
Event AuditMessage/ EventIdentification	EventID	M	EV(110107, DCM, "Import")
	EventActionCode	M	"C" (Create)
	EventDataTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	EV("ITI-14", "IHE Transactions", "Register Document Set")
Source (Document Repository or Integrated Document Source/Repository) (1)			
Destination (Document Registory) (1)			
Audit Source (Document Registory) (1)			
Patient (1)			
SubmissionSet (1)			

Where:

	Field Name	**Opt**	**Value Constraints**
Source AuditMessage/ ActiveParticipant	UserID	U	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"true"
	RoleIDCode	M	EV(110153, DCM, "Source")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name,

			"2" for IP adress
	NetworkAccessPointID	M	The machine name or IP adress, as specified in RFC 3881.
Destination AuditMessage/ ActiveParticipant	**Field Name**	**Opt**	**Value Constraints**
	UserID	U	SOAP endpoint URI
	AlternativeUserID	M	the process ID as used within the local operating system in the local system logs.
	UserName	U	not specialized
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV(110152, DCM, "Destination")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP adress
	NetworkAccessPointID	M	The machine name or IP adress, as specified in RFC 3881.
Audit Source AuditMessage/ AuditSource Identification	**Field Name**	**Opt**	**Value Constraints**
	AuditSourceID	U	not specialized
	AuditEnterpriseSiteID	U	not specialized
	AuditSourceTypeCode	U	not specialized
Patient AuditMessage/ ParticipantObject Identification	**Field Name**	**Opt**	**Value Constraints**
	ParticipantObjectTypeCode	M	"1" (person)
	ParticipantObjectTypeCodeRole	M	"1" (patient)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	the patient ID in HL7 CX format..
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
SubmissionSet AuditMessage/ ParticipantObject Identification	**Field Name**	**Opt**	**Value Constraints**
	ParticipantObjectTypeCode	M	"2" (System)
	ParticipantObjectTypeCodeRole	M	"20" (job)
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV("urn:uuid:a54d6aa5-d40d-43 f9-88c5-b4633d873bdd", "IHE XDS Metadata", "submission set classificationNode")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	the submissionSet unique ID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized

D.3　監査証跡ログのスキーマ

```
<!--  edited with XMLSPY v2004 rel. 3 U (http://www.xmlspy.com) by Glen F. Marshall (HL7 Technical Steering Committee)  -->
- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
- <xs:element name="AuditMessage">
- <xs:complexType>
- <xs:sequence>
<xs:element name="EventIdentification" type="EventIdentificationType" />
- <xs:element name="ActiveParticipant" maxOccurs="unbounded">
- <xs:complexType>
- <xs:complexContent>
<xs:extension base="ActiveParticipantType" />
</xs:complexContent>
</xs:complexType>
</xs:element>
<xs:element name="AuditSourceIdentification" type="AuditSourceIdentificationType" maxOccurs="unbounded" />
<xs:element name="ParticipantObjectIdentification" type="ParticipantObjectIdentificationType" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
</xs:complexType>
</xs:element>
- <xs:complexType name="EventIdentificationType">
- <xs:sequence>
<xs:element name="EventID" type="CodedValueType" />
<xs:element name="EventTypeCode" type="CodedValueType" minOccurs="0" maxOccurs="unbounded" />
</xs:sequence>
- <xs:attribute name="EventActionCode" use="optional">
- <xs:simpleType>
- <xs:restriction base="xs:string">
- <xs:enumeration value="C">
- <xs:annotation>
<xs:appinfo>Create</xs:appinfo>
</xs:annotation>
</xs:enumeration>
- <xs:enumeration value="R">
- <xs:annotation>
<xs:appinfo>Read</xs:appinfo>
</xs:annotation>
</xs:enumeration>
- <xs:enumeration value="U">
- <xs:annotation>
<xs:appinfo>Update</xs:appinfo>
</xs:annotation>
</xs:enumeration>
- <xs:enumeration value="D">
- <xs:annotation>
<xs:appinfo>Delete</xs:appinfo>
</xs:annotation>
</xs:enumeration>
- <xs:enumeration value="E">
- <xs:annotation>
<xs:documentation>Execute</xs:documentation>
</xs:annotation>
</xs:enumeration>
</xs:restriction>
</xs:simpleType>
```

```
    </xs:attribute>
    <xs:attribute name="EventDateTime" type="xs:dateTime" use="required" />
  - <xs:attribute name="EventOutcomeIndicator" use="required">
  - <xs:simpleType>
    - <xs:restriction base="xs:integer">
      - <xs:enumeration value="0">
        - <xs:annotation>
            <xs:appinfo>Success</xs:appinfo>
          </xs:annotation>
       </xs:enumeration>
      - <xs:enumeration value="4">
        - <xs:annotation>
            <xs:appinfo>Minor failure</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="8">
      - <xs:annotation>
          <xs:appinfo>Serious failure</xs:appinfo>
        </xs:annotation>
       </xs:enumeration>
      - <xs:enumeration value="12">
        - <xs:annotation>
            <xs:appinfo>Major failure; action made unavailable</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
       </xs:restriction>
      </xs:simpleType>
     </xs:attribute>
  </xs:complexType>
- <xs:complexType name="AuditSourceIdentificationType">
  - <xs:sequence>
     <xs:element name="AuditSourceTypeCode" type="CodedValueType" minOccurs="0"
     maxOccurs="unbounded" />
      </xs:sequence>
      <xs:attribute name="AuditEnterpriseSiteID" type="xs:string" use="optional" />
      <xs:attribute name="AuditSourceID" type="xs:string" use="required" />
   </xs:complexType>
  - <xs:complexType name="ActiveParticipantType">
  - <xs:sequence minOccurs="0">
     <xs:element name="RoleIDCode" type="CodedValueType" minOccurs="0"
       maxOccurs="unbounded" />
     </xs:sequence>
     <xs:attribute name="UserID" type="xs:string" use="required" />
     <xs:attribute name="AlternativeUserID" type="xs:string" use="optional" />
     <xs:attribute name="UserName" type="xs:string" use="optional" />
     <xs:attribute name="UserIsRequestor" type="xs:boolean" use="optional" default="true" />
     <xs:attribute name="NetworkAccessPointID" type="xs:string" use="optional" />
  - <xs:attribute name="NetworkAccessPointTypeCode" use="optional">
     - <xs:simpleType>
       - <xs:restriction base="xs:unsignedByte">
          - <xs:enumeration value="1">
           - <xs:annotation>
              <xs:appinfo>Machine Name, including DNS name</xs:appinfo>
            </xs:annotation>
          </xs:enumeration>
        - <xs:enumeration value="2">
        - <xs:annotation>
            <xs:appinfo>IP Address</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
       - <xs:enumeration value="3">
          - <xs:annotation>
          <xs:appinfo>Telephone Number</xs:appinfo>
```

```
          </xs:annotation>
         </xs:enumeration>
        </xs:restriction>
       </xs:simpleType>
      </xs:attribute>
     </xs:complexType>
  - <xs:complexType name="ParticipantObjectIdentificationType">
- <xs:sequence>
     <xs:element name="ParticipantObjectIDTypeCode" type="CodedValueType" />
- <xs:choice minOccurs="0">
     <xs:element name="ParticipantObjectName" type="xs:string" minOccurs="0" />
     <xs:element name="ParticipantObjectQuery" type="xs:base64Binary" minOccurs="0" />
    </xs:choice>
   <xs:element name="ParticipantObjectDetail" type="TypeValuePairType" minOccurs="0"
     maxOccurs="unbounded" />
   </xs:sequence>
  <xs:attribute name="ParticipantObjectID" type="xs:string" use="required" />
   - <xs:attribute name="ParticipantObjectTypeCode" use="optional">
- <xs:simpleType>
   - <xs:restriction base="xs:unsignedByte">
    - <xs:enumeration value="1">
     - <xs:annotation>
         <xs:appinfo>Person</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
    - <xs:enumeration value="2">
     - <xs:annotation>
        <xs:appinfo>System object</xs:appinfo>
         </xs:annotation>
       </xs:enumeration>
    - <xs:enumeration value="3">
      - <xs:annotation>
          <xs:appinfo>Organization</xs:appinfo>
       </xs:annotation>
       </xs:enumeration>
    - <xs:enumeration value="4">
      - <xs:annotation>
         <xs:appinfo>Other</xs:appinfo>
        </xs:annotation>
       </xs:enumeration>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
   - <xs:attribute name="ParticipantObjectTypeCodeRole" use="optional">
- <xs:simpleType>
   - <xs:restriction base="xs:unsignedByte">
    - <xs:enumeration value="1">
     - <xs:annotation>
        <xs:appinfo>Patient</xs:appinfo>
      </xs:annotation>
       </xs:enumeration>
    - <xs:enumeration value="2">
     - <xs:annotation>
         <xs:appinfo>Location</xs:appinfo>
       </xs:annotation>
      </xs:enumeration>
    - <xs:enumeration value="3">
     - <xs:annotation>
       <xs:appinfo>Report</xs:appinfo>
       </xs:annotation>
      </xs:enumeration>
    - <xs:enumeration value="4">
     - <xs:annotation>
```

```
        <xs:appinfo>Resource</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="5">
    - <xs:annotation>
        <xs:appinfo>Master file</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="6">
    - <xs:annotation>
        <xs:appinfo>User</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="7">
    - <xs:annotation>
        <xs:appinfo>List</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="8">
    - <xs:annotation>
        <xs:appinfo>Doctor</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="9">
    - <xs:annotation>
        <xs:appinfo>Subscriber</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="10">
    - <xs:annotation>
        <xs:appinfo>Guarantor</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="11">
    - <xs:annotation>
        <xs:appinfo>Security User Entity</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="12">
    - <xs:annotation>
        <xs:appinfo>Security User Group</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="13">
    - <xs:annotation>
        <xs:appinfo>Security Resource</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="14">
    - <xs:annotation>
        <xs:appinfo>Security Granualarity Definition</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="15">
    - <xs:annotation>
        <xs:appinfo>Provider</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  - <xs:enumeration value="16">
    - <xs:annotation>
        <xs:appinfo>Report Destination</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
```

```
      - <xs:enumeration value="17">
        - <xs:annotation>
            <xs:appinfo>Report Library</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="18">
        - <xs:annotation>
            <xs:appinfo>Schedule</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="19">
        - <xs:annotation>
            <xs:appinfo>Customer</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="20">
        - <xs:annotation>
            <xs:appinfo>Job</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="21">
        - <xs:annotation>
            <xs:appinfo>Job Stream</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="22">
        - <xs:annotation>
            <xs:appinfo>Table</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="23">
        - <xs:annotation>
            <xs:appinfo>Routing Criteria</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
        - <xs:enumeration value="24">
          - <xs:annotation>
              <xs:appinfo>Query</xs:appinfo>
            </xs:annotation>
          </xs:enumeration>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
- <xs:attribute name="ParticipantObjectDataLifeCycle" use="optional">
  - <xs:simpleType>
    - <xs:restriction base="xs:unsignedByte">
      - <xs:enumeration value="1">
        - <xs:annotation>
            <xs:appinfo>Origination / Creation</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="2">
        - <xs:annotation>
            <xs:appinfo>Import / Copy from original</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="3">
          - <xs:annotation>
              <xs:appinfo>Amendment</xs:appinfo>
            </xs:annotation>
          </xs:enumeration>
      - <xs:enumeration value="4">
        - <xs:annotation>
```

```
            <xs:appinfo>Verification</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="5">
        - <xs:annotation>
            <xs:appinfo>Translation</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="6">
      - <xs:annotation>
            <xs:appinfo>Access / Use</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="7">
        - <xs:annotation>
            <xs:appinfo>De-identification</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="8">
        - <xs:annotation>
            <xs:appinfo>Aggregation, summarization, derivation</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
      - <xs:enumeration value="9">
        - <xs:annotation>
            <xs:appinfo>Report</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
    - <xs:enumeration value="10">
      - <xs:annotation>
            <xs:appinfo>Export / Copy to target</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
    - <xs:enumeration value="11">
      - <xs:annotation>
            <xs:appinfo>Disclosure</xs:appinfo>
          </xs:annotation>
      </xs:enumeration>
    - <xs:enumeration value="12">
      - <xs:annotation>
            <xs:appinfo>Receipt of disclosure</xs:appinfo>
          </xs:annotation>
        </xs:enumeration>
    - <xs:enumeration value="13">
      - <xs:annotation>
            <xs:appinfo>Archiving</xs:appinfo>
          </xs:annotation>
      </xs:enumeration>
    - <xs:enumeration value="14">
      - <xs:annotation>
            <xs:appinfo>Logical deletion</xs:appinfo>
          </xs:annotation>
      </xs:enumeration>
    - <xs:enumeration value="15">
      - <xs:annotation>
            <xs:appinfo>Permanent erasure / Physical destruction</xs:appinfo>
        </xs:annotation>
          </xs:enumeration>
      </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="ParticipantObjectSensitivity" type="xs:string" use="optional" />
</xs:complexType>
```

```
 - <xs:complexType name="CodedValueType">
      <xs:attribute name="code" type="xs:string" use="required" />
      <xs:attributeGroup ref="CodeSystem" />
      <xs:attribute name="displayName" type="xs:string" use="optional" />
      <xs:attribute name="originalText" type="xs:string" use="optional" />
   </xs:complexType>
 - <xs:complexType name="TypeValuePairType">
      <xs:attribute name="type" type="xs:string" use="required" />
      <xs:attribute name="value" type="xs:base64Binary" use="required" />
   </xs:complexType>
 - <xs:attributeGroup name="CodeSystem">
      <xs:attribute name="codeSystem" type="OID" use="optional" />
      <xs:attribute name="codeSystemName" type="xs:string" use="optional" />
   </xs:attributeGroup>
 - <xs:simpleType name="OID">
- <xs:restriction base="xs:string">
      <xs:whiteSpace value="collapse" />
   </xs:restriction>
  </xs:simpleType>
 </xs:schema>
```

附属書 E.　オープンソースの利用方法

本附属書では、地域医療連携情報システムの実装に参考になる IHE 関連技術のオープンソースについて紹介する。

E.1　概要

これまで、さまざまな組織が IHE テクニカルフレームワークに従って XDS、PIX/PDQ などを実装してきた。これらの実装のうち、いくつかはオープンソースとして公開されている。これらのオープンソースは以下の点において期待できる。

・ 開発した各アクタの動作試験
・ オープンソースをベースとしたシステム開発に利用可能
・ 地域医療連携システムを構築する上での参考となる

そこで本章では、公開されているオープンソースのうち、

・ IHE が公開しているスキーマファイル
・ NIST　XDS レジストリ・リポジトリ
・ NIST　XDS ツールキット

を紹介する。さらに他のオープンソースに関する情報も提供する。

本附属書は実際に地域連携システムの開発を担当する技術者を対象とするが、Windows あるいは Linux の操作にある程度親しみ、オープンソースのインストール経験がある方であれば、実際にインストールし、動作させることができると思われる。興味のある方はお手持ちのマシンにぜひオープンソースをインストールし、動かして見ることをお勧めする。

なお、本書の内容は、2010 年 3 月現在の情報に基づく。

E.2　スキーマファイル

IHE では、XDS.b、XCA、PIX(HL7ver.3)、PDQ(HL7ver.3)の開発に有用なスキーマファイル（XSD ファイル）や WSDL 定義ファイルを公開している。以下の FTP サイト（図 E-1）から取得できる。

ftp://ftp.ihe.net/TF_Implementation_Material/ITI/packages

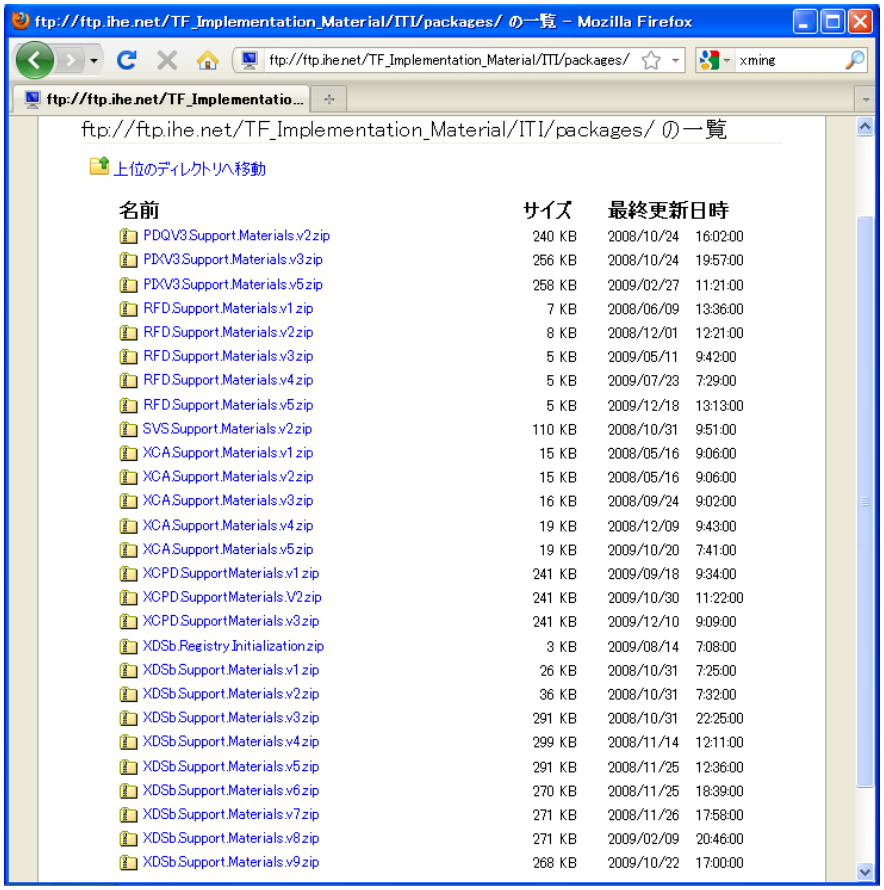


図 E-1　IHE スキーマファイル FTP サイト

このサイトにはさまざまな種類のファイルがあるが、XDS.b の各アクタを構築する場合は、このサイトから XDSb.Support.Materials.v9.zip をダウンロードする。

ダウンロードしたファイルを適当なディレクトリで展開すると、そのディレクトリに examples、schema、wsdl の 3 つのディレクトリができる。XSD ファイルは schema 以下に、WSDL 定義ファイルは wsdl 以下にそれぞれ格納されている。これらの XSD ファイル、WSDL ファイルを利用して、各アクタのインタフェース部分を構築することができる。しかし他に必要となる各アクタの機能は、IHE テクニカルフレームワークに従い別途実装する必要がある。

E.3　NIST　XDS レジストリ・リポジトリ

E.3.1　概要

本節では、アメリカ国立技術研究所(National Institute of Standards and Technology ： NIST)により開発・公開されている XDS レジストリ・リポジトリを紹介する。これは、XDS のドキュメントレジストリ及びドキュメントリポジトリがインタフェース部分も含め、テクニカルフレームワークに従って実装されたオープンソースである。また、XDS.b のほか、XDS.a にも対応している。

本オープンソースにより構築した XDS レジストリ・リポジトリサーバの概略を図 E-2 に示す。本サーバは Tomcat1 と Tomcat2 の 2 台の Tomcat サーバが連携して動作する。

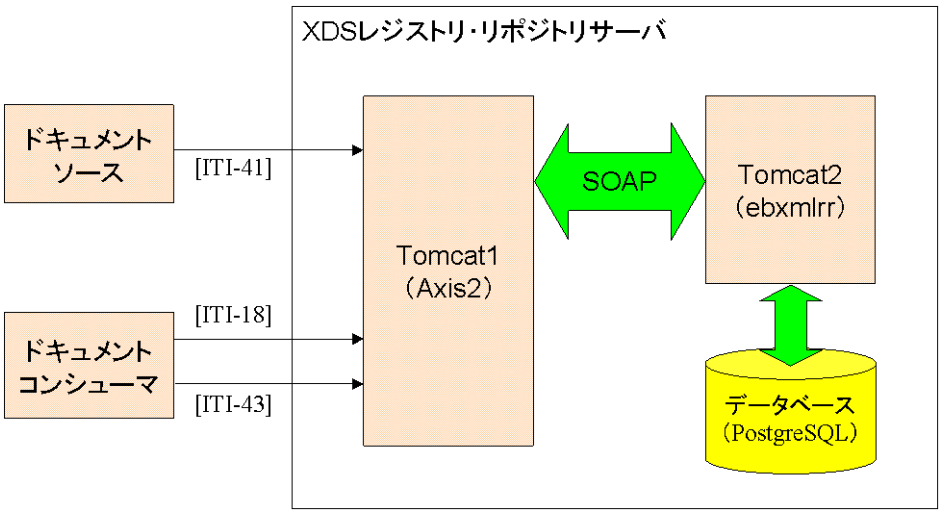


図 E-2 XDS レジストリ･リポジトリ概略図

Tomcat2 側は ebXML に基づくレジストリ・リポジトリが実装されたオープンソースである ebxmlrr のサーバとして動作する。なお ebxmlrr は ebXMLver2.0 に基づいて実装されている。

そのため Tomcat1 側では、XDS で定義されている処理と ebXML のバージョンの違いを吸収する処理を行う。具体的には以下を行う。

- ドキュメントソース及びドキュメントリポジトリとのインタフェース
- ドキュメントリポジトリ
- ドキュメントレジストリで行うメタデータ登録に関するすべての処理（ただしメタデータの保存は ebxmlrr で行う）
- ドキュメントコンシューマからストアドクエリを受け取ったとき、それに対応する SQL クエリを作成する（クエリの変換）。
- XDS.b に対応するためのメタデータの形式変換（ebXMLver3.0 と ebXMLver2.0 との間のバージョンの違いによるメタデータの変換）。

E.3.2 あらかじめ必要となるツール

本オープンソースは Linux 上で動作し、インストールに際して以下のものが必要となる。

- Sun Java ：JDK1.5
- PostgreSQL 8

なお、Tomcat、Axis、ebxmlrr はダウンロードパッケージに含まれる。さらにソースコードを取得する場合は以下のツールも必要となる。

- ant
- Subversion (SVN)

E.3.3　ダウンロード及びインストール

オープンソースのダウンロード及びインストールの方法は、以下のサイト（IheOs Installation：図 E-3）に説明されている（ただし説明は英語である）。

http://ihexds.nist.gov/XdsDocs/opensource/install.html

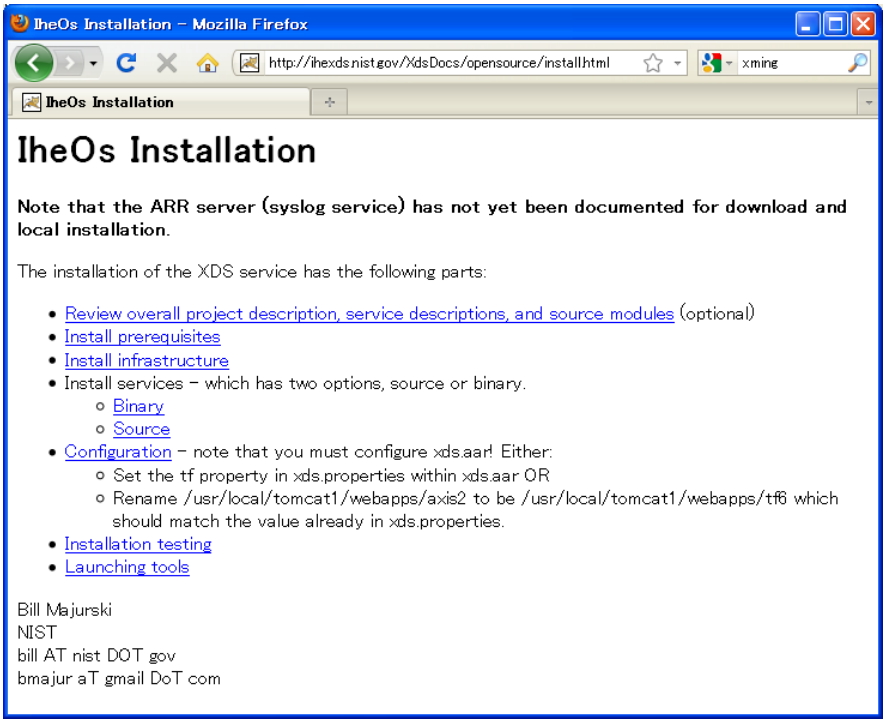


図 E-3　IheOs Installation

上記マニュアルに沿ってインストールが終了したならば、PostgreSQL を起動している状態で２つの Tomcat を起動させれば､外部からの要求待ち状態になる。

E.3.4　その他の機能

本節で紹介した XDS レジストリ・リポジトリには、本来のドキュメントレジストリ、ドキュメントリポジトリとしての機能の他に、以下の機能もある。

（１）患者 ID の簡易割り当て機能

本節で紹介した XDS レジストリ・リポジトリにドキュメントの登録を行う場合、あらかじめ Web ブラウザなどで下記サイトにアクセスして患者 ID を取得しておく。ただし、下記サイトのアドレスにある<ホスト名>は XDS レジストリ・リポジトリをインストールしたマシンのホスト名である（IP アドレスでもよい）。Web ブラウザを動作させるマシンに XDS レジストリ・リポジトリをインストールされている場合ならば localhost としてよい。

http://<ホスト名>:9080/xdstools/pidallocate [6]

上記サイトにアクセスすると、図 E-4 のようにブラウザ上に表示される。

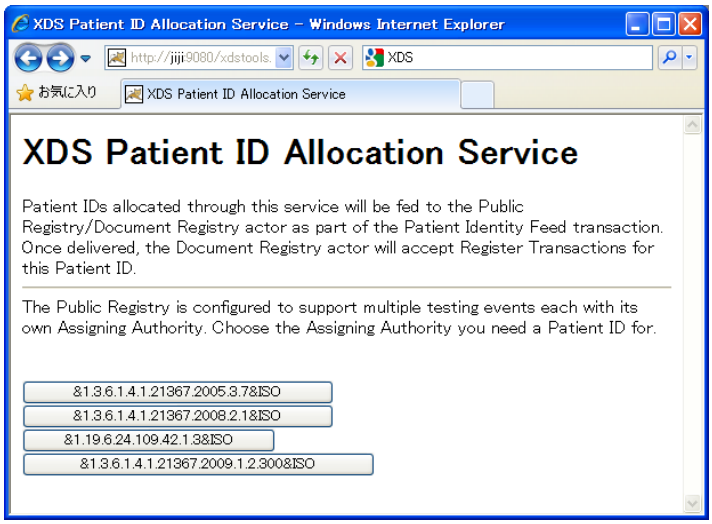


図 E-4 XDS 患者 ID 割り当てサイト

図 E-4 では AssigningAuthority のボタンが４つ用意されている。たとえば一番上のボタンを押下すると、ブラウザには図 E-5 のように表示される。図 E-5 にある「d6a1818b2cd9446^^^&1.3.6.1.4.1.21367.2005.3.7&ISO」が割り当てられた患者 ID となる。

[6] 2010 年 3 月時点での最新版(ダウンロードファイル名：xds_06_09.tgz)をインストールして、患者 ID の割り当てサイトにアクセスすると、「例外」として web ブラウザ上に以下のメッセージが表示される。

javax.servlet.ServletException: サーブレットクラス gov.nist.registry.xdstools.servlet.PidAllocateServlet を初期化中にエラーが発生しました。

さらに同じ web ブラウザ上にその「原因」として、

java.lang.NoClassDefFoundError: gov/nist/registry/common2/exception/XdsInternalException

と表示される。これは本来必要とされるパッケージがダウンロードしたものから欠落しているのが原因である。これを回避して図E-4を表示させるためには、/usr/local/tomcat1/webapps/xdstools/WEB-INF/lib に xds-common.jar と xdsLog.jar をコピーした上で、tomcat1 を再起動する。なお xds-common.jar と xdsLog.jar は/usr/local/tomcat1/webapps/LogReader/WEB-INF/lib に含まれている。

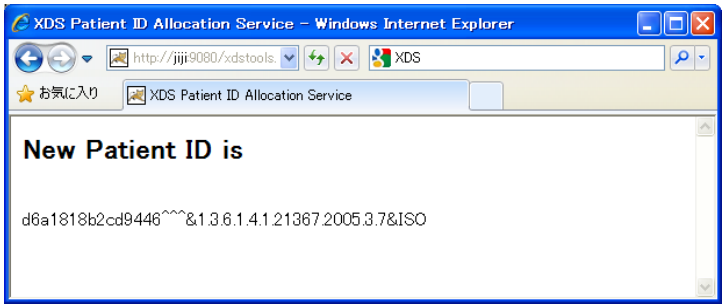


図 E-5　患者 ID の割り当て

ドキュメント登録を行う利用者は、上記サイトから取得した患者 ID をドキュメントエントリ、フォルダ、サブミッションセットの属性である PatientID として設定する。

また、この患者 ID はサーバ側のデータベースに保存され、ドキュメント登録実行時にレジストリ側で行われるメタデータの検証での患者 ID のチェックで利用される。

（２）LogRoader

ドキュメントの登録・検索・取得処理の受付、実行において、XDS レジストリ・リポジトリサーバはログを出力する。出力されたログはデータベースへ蓄積されるが、これらのログを閲覧するツールとして、LogReader が用意されている。任意の Web ブラウザにおいて、以下のアドレスへ接続する。

http://<サーバ名>:9080/LogReader

図 E-6 に LogReader 画面を示す。図の左側にログの一覧が表示され、その中から一つ選択すると、ログの詳細がブラウザの右側に表示される。

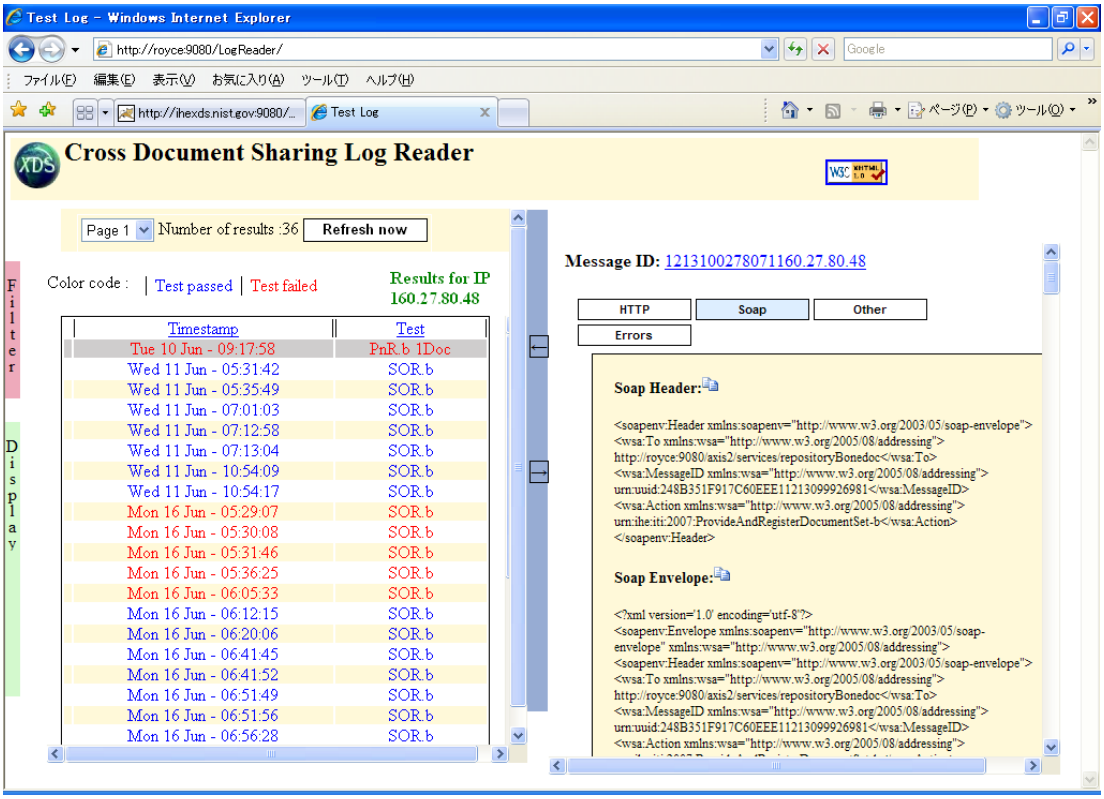


図 E-6 LogReader

（3）XDS Viewer

XDS Viewer を利用することで XDS レジストリ・リポジトリへ登録されたメタデータを検索・閲覧が可能である。任意の Web ブラウザで以下のサイトへ接続する。

http://<ホスト名>:9080/xdstools/viewer

図 E-7 に接続直後にブラウザ上に表示されたものを示す。

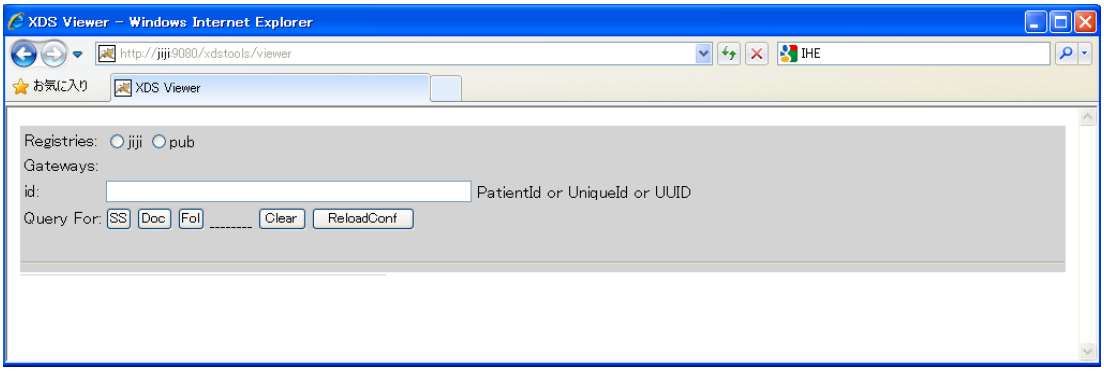


図 E-7 XDS Viewer 初期画面

図 E-7 の画面で、接続先レジストリを選択し、検索条件として患者 ID、ユニーク ID、UUID のいずれかを入力する。その後メタデータの種類（SS：SubmissionSet、Doc：DocumentEntry、Fol：Folder）のボタンを押下すると、検索を開始する。検索の結果は図 E-8 左下に一覧表示される（図 E-8 の表示は図 E-7 で「SS」ボタンを押下した時）。表示項目にはいくつかのリンクがあるが、これらを押下するとリンクに応じた詳細情報が図 E-8 右側に表示される。図 E-8 は図中左側にあるリンク「SS1」を押下したとき、図中右側に登録された SubmissionSet の属性値が表示されたときのものである。

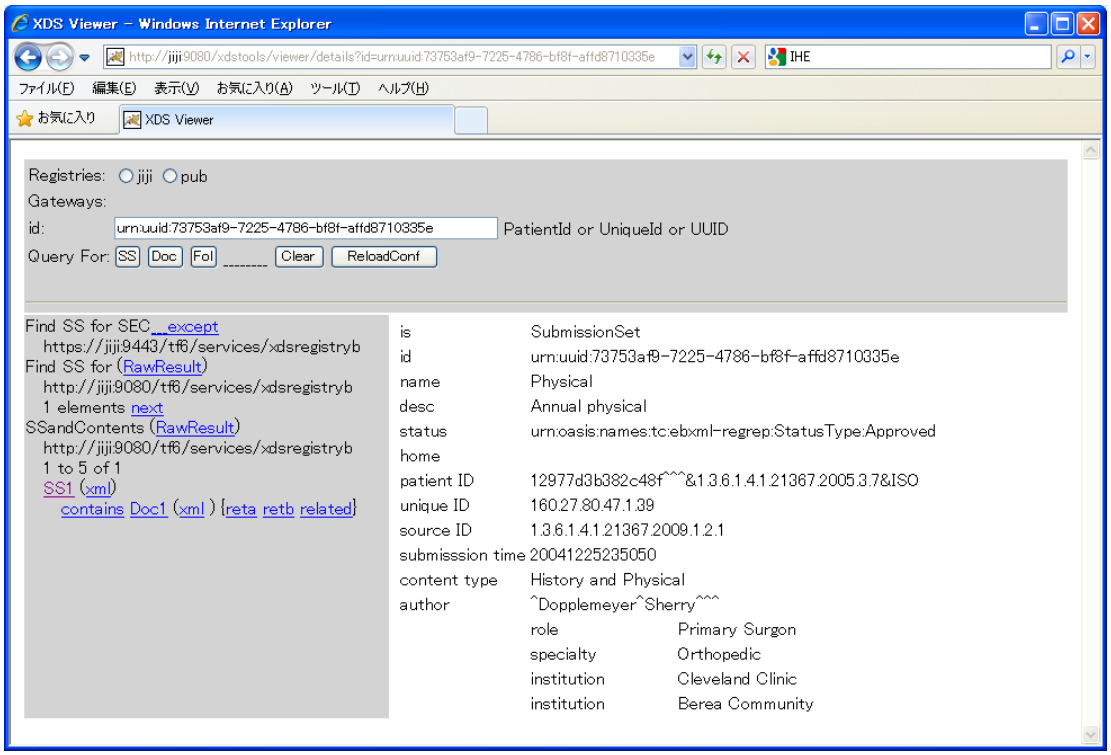


図 E-8 XDS Viewer

E.3.5 Public Registry

NIST では、XDS レジストリ・リポジトリをオープンソースとして公開するだけでなく、サーバマシンにインストールして、Public Registry としてインターネット上に外部公開している。Public Registry はその利用に際して特別な手続きは必要なく、自由に利用できる。そのため後述の XDS ツールキットで Public Registry にアクセスして各種動作を確認したり、開発したドキュメントソース及びドキュメントコンシューマの動作試験に利用したりすることができる。

Public Registry については、以下のサイトを参照のこと。下記サイトに Public Registry へアクセスするためのエンドポイント URL が記載されている。

http://ihewiki.wustl.edu/wiki/index.php/XDS_Main_Page#Public_Registr

y_Server_Configuration

E.4 XDS ツールキット

E.4.1 概要

XDS ツールキットは、XDS におけるドキュメントリポジトリ及びドキュメントリポジトリの動作試験を行う目的で公開されているテストツールである。試験対象となるアクタがドキュメントレジストリの場合、XDS ツールキットはドキュメントリポジトリ及びドキュメントコンシューマの役割を持つ。またドキュメントリポジトリが試験対象となる場合は、XDS ツールキットはドキュメントソース及びドキュメントコンシューマの役割を果たす。

E.4.2 あらかじめ必要となるツール

XDS ツールキットは Windows 及び Linux で動作し、Sun の Java（JDK1.5）があらかじめインストールされている必要がある。

ただし XDS ツールキットは bash-shell 上で動作するため、Windows 上で利用するには、以下のうちの一つを別途インストールしておく必要がある。

- cygwin
- win-bash
- GNU bash for Windows
- そのほか Windows 上で動作する bash-shell ツール

E.4.3 ダウンロード及びインストール

任意の Web ブラウザで以下のサイトへアクセスする。

http://ihexds.nist.gov/XdsDocs/xdstoolkit/

上記サイトへアクセスすると、図 E-9 に示すファイルのリストが表示される。ファイル名 xdstoolkit_XX_YY.zip をクリックすると XDS ツールキットのダウンロードが始まる。なお 2010 年 3 月 1 日時点での最新版は xdstoolkit_06_13.zip（図 E-9 の赤枠で囲んだ部分）である。そこで、以下の説明では xdstoolkit_06_13.zip に基づいて説明する。

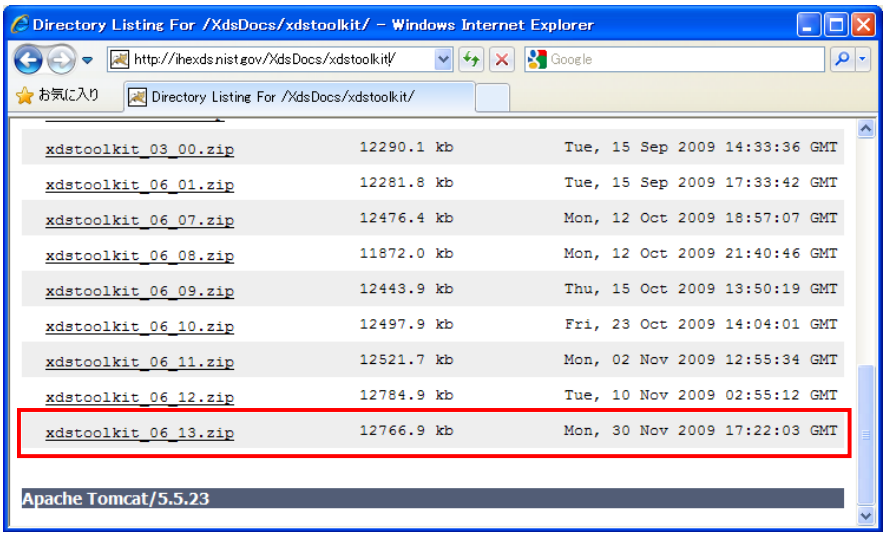


図 E-9 XDS ツールキットダウンロードサイト

取得したファイル xdstoolkit_06_13.zip を任意のディレクトリ<TestDir>で展開する。このとき、<TestDir>に xdstoolkit_06_13 というディレクトリができる。あと環境設定、パラメータ設定、テスト実行方法などの詳細な説明がディレクトリ<TestDir>/xdstoolkit_06_13/docs にある install.txt にあるので参照のこと。

E.4.4 テストに関する情報

XDS ツールキットが使用するテスト用データ、ならびにテスト用設定ファイルはディレクトリ<TestDir>/xdstoolkit_06_13/testkit 以下にある。ディレクトリ testkit には 14 個のディレクトリがあり、その中の５つのディレクトリ example、selftest、server、testdata、tests にはさらに 5 桁の数字が名前となるディレクトリが複数含まれている。

これらのディレクトリにはそれぞれテスト用データならびにテスト用設定ファイルが含まれている。またディレクトリの名前となっている 5 桁の数字がテスト番号である。このテスト番号の意味は、以下の（１）、（２）で説明される。

（１）Test Description

個々のテスト番号が指すテストの内容が、テスト番号順に説明されている。2009-2010 年度のテストについては以下のサイト

http://ihewiki.wustl.edu/wiki/index.php/XDS_Test_Kit_2009-2010_Test_Descriptions

を参照のこと。上記サイトでテスト番号 12049 の説明がある部分を図 E-10 に示す。

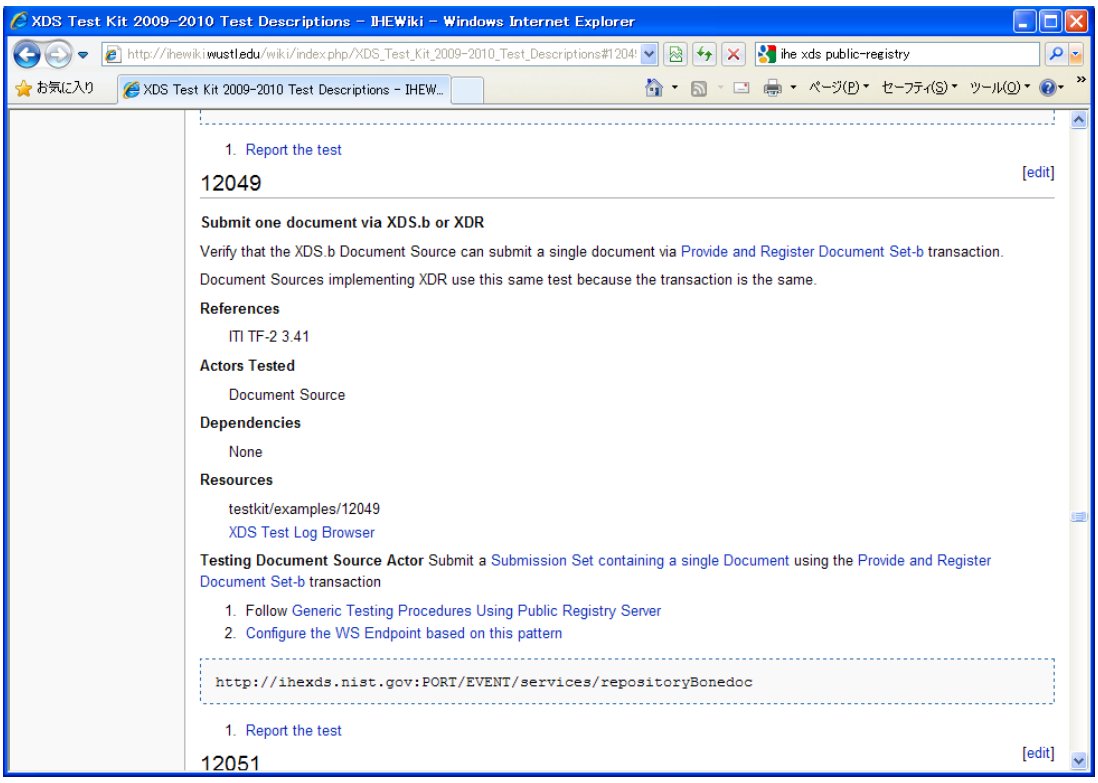


図 E-10 Test Description(テスト番号 12049)

（2）Test Requirements

各テストにおいて、どのアクタがテストの対象となっているか表す。以下のサイトにおいてはトランザクションごとに表としてまとめられている。

http://ihewiki.wustl.edu/wiki/index.php/XDS_Test_Kit_Test_Requirements

図 E-11 には、トランザクション Retrieve Document Set [ITI-43]において、その対象となるテスト番号、およびテストごとに試験対象となるアクタが表されている。テスト番号には Test Description へのリンクが張られており、テスト番号をクリックすることで該当のテストが説明されている場所へ遷移できるようになっている。

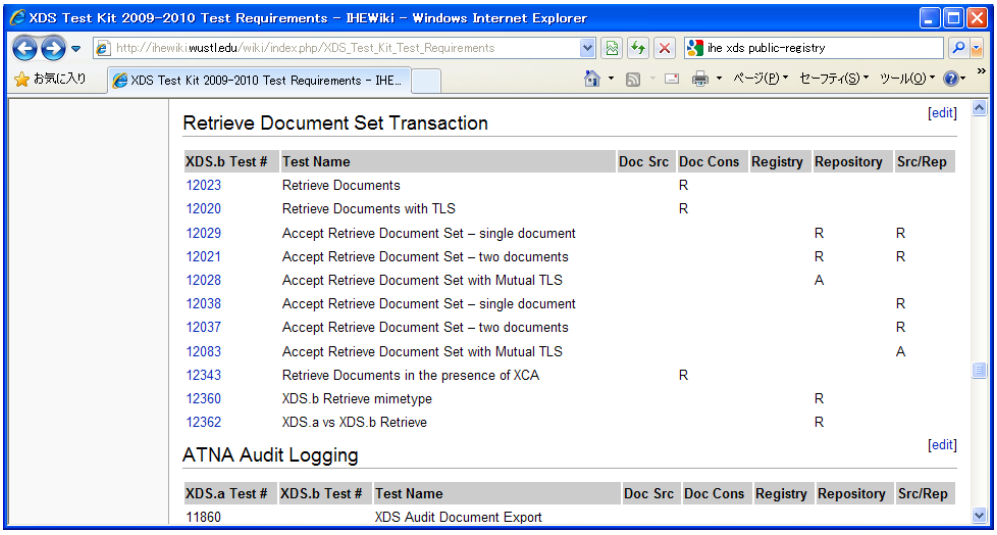


図 E-11 Test Requirements(トランザクション Retrieve Document Set)

例としてテスト番号 12029 (Accept Document Set - Single Document) では、リポジトリ(Repository)とソース・リポジトリ一体型(Src/Rep)で「R」となっているが、記号「R」は「必須 (Require)」を表し、テスト 12029 の試験対象であることを指す。

また、ドキュメントソース (Doc Src)、ドキュメントコンシューマ (Doc Cons) 及びドキュメントレジストリ (Registry) は空欄となっているが、これはテスト 12029 では、該当のアクタは試験対象でないことを表している。

表中の記号は「R」以外にも多様な記号が使われているが、記号の意味は上記サイト中に説明されている (図 E-12)。

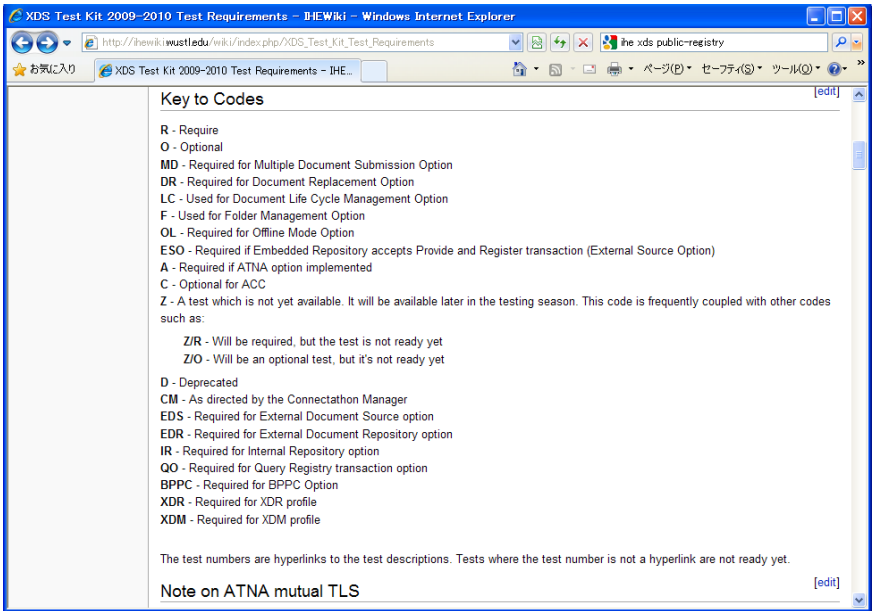


図 E-12 Test Requirements

E.5 他のオープンソース

本章で紹介したもの以外にも、地域連携システムの構築に利用可能なオープンソースが公開されている、そこで本節ではこれらを簡単に説明する。

E.5.1 OpenHealthTools が公開するオープンソース

OpenHealthTools(OHT)では、IHE テクニカルフレームワークに沿って PIX/PDQ、ATNA 及び XDS のサーバサイドを実装し、以下の名前でオープンソースとして公開している。

- openpixpdq
- openatna
- openxds

このうち、openatna と openxds はソースコードが Subversion (SVN) サーバ上で公開されている。従って取得のためにはあらかじめ Subversion クライアントツールのインストールが必要となる。

一方 OpenPIXPDQ はバイナリ版、ソースコード版の両方をダウンロードサイトから取得できるようになっている。

各オープンソースについての詳しい情報はそれぞれ、下記のサイトを参照のこと。システムの構造やインストール方法まで幅広く記述されている。

OpenPIXPDQ
https://openpixpdq.projects.openhealthtools.org/
OpenATNA
https://openatna.projects.openhealthtools.org/
OpenXDS
https://openxds.projects.openhealthtools.org/

E.5.2 CodePlex

CodePlex はマイクロソフト社が運営する開発プロジェクトのホスティング web サイトである。この開発プロジェクトの一つとして XDS.b が実装され、オープンソースとして公開されている。詳細は下記サイトを参照のこと。

http://ihe.codeplex.com/

E.5.3 Omar

NIST の XDS レジストリ・リポジトリ（E.3 参照）では、レジストリの中核部分として ebxmlrr を利用しているが、これは ebXML ver2.0 に基づいて実装されている。しかし、ebXML は現在 ver3.0 となっており、XDS.b で参照しているのはこのバージョンである。Omar (Object, Metadata and Artifacts Registry) はこの ebXML ver3.0 に基づいて実装されたオープンソースで、Sourceforge から公開されている（下記サイト）。

http://sourceforge.net/projects/ebxmlrr/files/

Sourceforge から公開されているものは java のソースコードであり、コンパイル、インストールの方法ならびに Omar に関するいろいろな情報は下記サイトから参照可能である。

http://ebxmlrr.sourceforge.net/
http://ebxmlrr.sourceforge.net/wiki/index.php/Main_Page　(Omar wiki)

XDS.b に基づくレジストリの開発においては、レジストリの中核部分として Omar が利用可能である。ただしメタデータの検証、ストアドクエリの取り扱い、フォルダの属性 lastUpdateTime の更新など、XDS.b で規定されている処理については別途実装が必要となる。

附属書 F.　IHE ポリシーTemplate など

本附属書では、第4章で紹介した「TI　User Handbooks」3文書の内容を概説する。

各文書は、医療連携コミュニティ(XAD)構築時に行うべきポリシー作成やリスク分析、合意文書作成指針について記載されている。実際の構築時には、基本的認識事項として便利に利用できる。

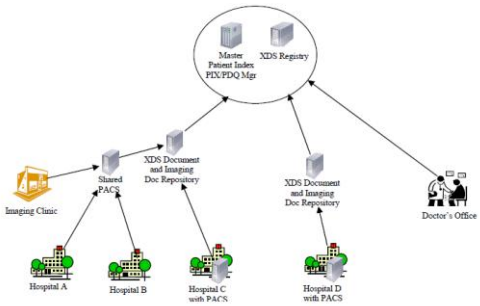
F.1　医療連携コミュニティの構築

医療連携コミュニティの構築

ーITI　User Handbooksー
Cookbook,HIE Security & Privacy,Template

附属書 F1
本文4章で紹介した「 ITI　User Handbooks」3文書の内容概説です。
各文書は、医療連携コミュニティ(XAD)構築時に行うべきポリシー作成やリスク分析、合意文書作成指針について記載されています。実際の構築時には、基本的認識事項として便利に利用が出来ます。

XADの構成



Example XDS Affinity Domain Architecture

IHE IT Infrastructure White Paper
HIE Security and Privacy through
IHE Profiles

Ver2.0 2008.Aug.22

contents

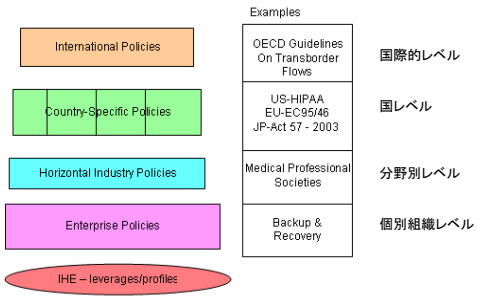
Introduction & Scope

・HIE(healthcare Information Exchange)は、複数医療機関が一人の患者の診療情報を長期に共有する仕組み。
・ドキュメントは、単純なテキスト文書(Ex.PDF)や標準的構造文書(Ex.HL7 CDA)。
・HIEの構成員は、基本的なセキュリティ原理を実装する必要がある。
・HIEは、XDSを中心とするプロファイルで構成される。
・IHE based HIEが、患者のプライバシーと情報セキュリティを守るため技術だけでなく、ポリシー定義が重要。
・IHEのプロファイルは、相互運用性の確保に必要な技術的詳細の取決め。
　Privacy and Security Polices、Risk Management、Operating Systems、Healthcare Application Functionality、Physical Controls、general Network Controlsについては触れていない。
・Templateは概要を示す。

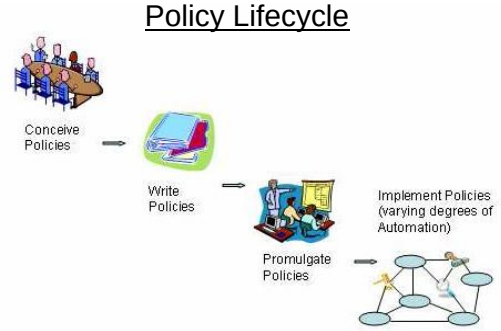
・本White Paperはプライバシとセキュリティのために、IHEプロファイルの使い方を示す。
・Risk Management実施には本ガイドを取り入れることがシステム実装者の義務。

Policy environment

ポリシー環境は多層になっている



Policy Lifecycle



Policies

実システムでは多くのポリシーを調和させる必要がある。

a) アクセスできる資格とHIE文書
b) HIEとしての提供できる文書
c) HIEとして受け入れられる文書タイプ
d) HIEとして受容可能なリスクレベル
e) HIEポリシーの違反者への制裁
f) 訓練と周知
g) 加入と脱退
h) 非常時の運用
i) 許されるNW使用と防御
j) 認証手段
k) バックアップと回復
l) 第三者の許容アクセス
m) HIE情報の二次利用
n) HIEの可用性 (life critical, normal, or low priority)
o) 保守
p) HIEでのデータ保持期間

これらのポリシーは、対等ではなく上下関係がある。
(社会的一般規約 ⇒個別施設の規約 ⇒個々の事情による変更)

Emergency Mode

・Emergencyの定義は広い
・Emergency時にポリシーを緩めることは合理的
・Emergency時のポリシーは重要
・Emergencyとは
a) 自然・人的災害(例. Hurricane, Earth Quake)
 – 他地域からの応援救助者による迅速なアクセス
b) ユーティリティの不調(例. 停電)
 – 無停電電源、バックアップ電源
c) IT インフラの不調(例. hard drive crash)
 – 基本インフラ部分の冗長化
d) 患者緊急時の特権的行為
 – ブレークグラス(例.看護師による薬剤処方)
e) 患者の顕著な危機に対してのアクセス防御の無視
 – ポリシーに明示されることで、ポリシー違反にあたらない
Policy同士の衝突があるが、表面的。
欧州では「人種」の記載は禁止されてるが、診療上は重要
⇒ 「遺伝子情報の記録」として可とされる。

Technical Security and Privacy controls

一般的なSecurity and Privacy controls はOECDの原則によって公表されている。
security and privacy controls には、下記のことが用いられる。

1) 責任管理(Accountability Controls)
 – 例: security audit logging, reporting, alerting and alarming.
2) 本人特定と認証(Identification and Authentication Controls)
 – 例: personal interactions, Digital Certificates, security assertions, Kerberos, and LDAP.
3) アクセス制御(Access Controls)
 – 例: Role Based Access Controls.
4) 秘匿性(Confidentiality Controls)
 – 例:encryption or access controls.
5) 完全性(Data Integrity Controls)
 – 例: digital signatures, secure hash algorithms, CRC, and checksum.
6) 否認防止(Non-Repudiation Controls)
7) 患者プライバシ(Patient Privacy Controls)
8) 可用性(Availability Controls)
 –例: backup, replication, fault tolerance, RAID, trusted recovery, uninterruptible power supplies, etc.

例: OECD原則におけるデータ保護の2原則

◆安全管理の原則:
◎見せるべきではない人には開示しない
・Identification and Authentication Controls.
・Access Controls.
・Confidentiality Controls.
・患者プライバシ管理
◎無権限者による変更禁止
・Identification and Authentication Controls.
・Access Controls
・Data Integrity Controls.
◎必要時のアクセスの確保
・Availability Controls
◆責任の原則:
◎行為主体者の確認
・Identification and Authentication Controls.
◎行為者と内容
・Accountability Controls.
◎行為の否定不可
・Non-Repudiation Controls

このsecurity and privacy controlsには、各種ポリシーによる入力が要る。
IHEプロファイルが適用できる

Patient Privacy Consent(BPPC)

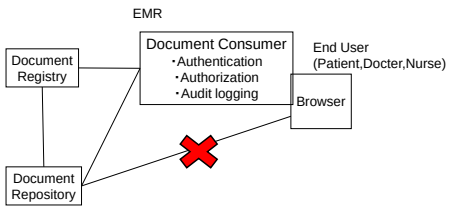
◆患者同意の標準はOASIS、HL7、ISO、ASTM等で開発している。
◆BPPCは拡張中であり粗いレベルだが、多くの場合で充分である。
HIEへのゲートキーパーになりうる。
◆BPPCによって可能になるポリシーは、
・明示的に Opt-In :患者による HIEで使用可能な文書の選択
・明示的に Opt-Out :患者による共有させない文書の選択
・暗黙的に Opt-In :許される文書用途
・明示的に Opt-Out :文書の公開
・明示的に Opt-Out :通常時のケアのための文書共有
・明示的に Opt-Out :非常時を含むケアのための文書共有
・明示的な取得認可 :特別な研究用途
・同意ポリシーの変更
・公開しない直接利用
・XCAによる文書使用の可能性
・明示的に Opt-in する個別ポリシー:各ケアイベントの都度
・明示的に特定のデータ利用

Access Control Policies の例

Sensitivity / Functional Role	Billing Information	Administrative Information	Dietary Restrictions	General Clinical Information	Sensitive Clinical Information	Research Information	Mediated by Direct Care Provider
Administrative Staff	X	X					
Dietary Staff		X	X				
General Care Provider		X	X	X			
Direct Care Provider		X	X	X	X		X
Emergency Care Provider		X	X	X	X		X
Researcher						X	
Patient or Legal Representative	X	X	X	X	X		

XDS の文書には様々なタイプ(doctype)があり、守秘レベル(confidentiality code)も役割によって分かれる(Role-Based Access Control)。

Authentication & Authorization



アクセス制御にはtopic of consent、confidentiality code、user、functional role、situation などの要素があるがこれが全てではない。現在の標準規約とはギャップがある。
IHEはpilot projectを行い、Security and Privacy modelの拡張でギャップを埋めていく。

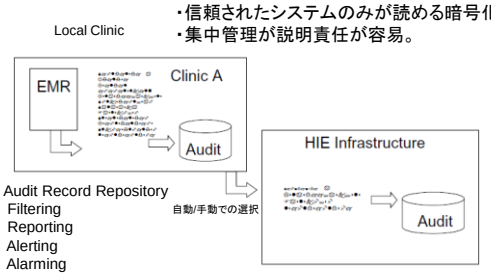
IHE security & privacy toolkit

IHEモデルはアプリケーション間の相互接続を定義。
アプリケーションの動作、機能、ポリシーは定義していない。

- Audit Trail and Node Authentication (ATNA)
- Consistent Time (CT)
- Basic Patient Privacy Consents (BPPC)
- Enterprise User Authentication (EUA)
- Cross-Enterprise User Assertion (XUA)
- Personnel White Pages (PWP)
- Digital Signatures (DSG)
- Notification of Document Availability (NAV)
- Cross-Enterprise Document Sharing (XDS)
- Cross-Enterprise Document sharing via Reliable messaging (XDR)
- Cross-Enterprise Document sharing on Media (XDM)

Audit flowdown

・ATNAは説明責任強化の基本。
ユーザ認証とアクセス制御、監査ログ、NW上の認証。
・信頼されたシステムのみが読める暗号化。
・集中管理が説明責任が容易。



統合プロファイルとセキュリティ確保

	説明性	認証	アクセス	秘匿	完全性	否認拒否	個人情報保護	利用性
ATNA（監査証跡とノード認証）	直	直	直	直	直	直	直	
BPPC（患者同意）				間			直	
CT（時刻の整合性）	直	間				直		
EUA（施設内ユーザ認証）	間	直	間	間		間	間	
XUA（施設間ユーザ認証）	間	直	間	間		間	間	
DSG（電子署名）	直	直			直	直		
XDS				直	直		間	直
XDR				直	直		間	直
XDM			間	直	直		間	直
PWP（職員の台帳）	間	直	直			間		

Cookbook: Preparing the IHE Profile Security Section

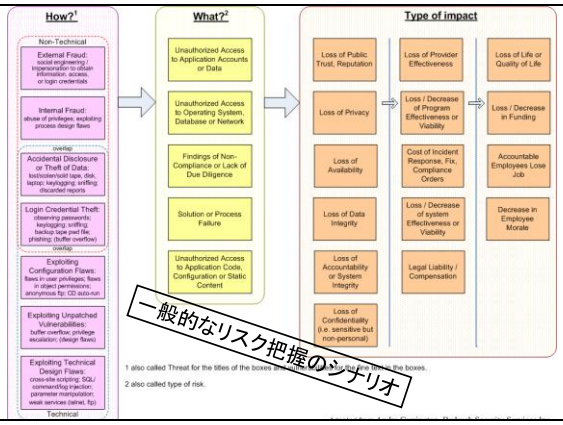
(Risk Management in Healthcare IT Whitepaper)

October 10, 2008

Risk assessment and mitigation table

Characterization of risks			Assessment of risks		Mitigation of risks			
Scenario	Asset	Type of impact	Level of impact	Probability	Mitigation	New level of impact	New probability	Comments

この表を使用して、以下のステップを行う。
①リスクの把握を行い
②リスクのimpactとlikelihoodを評価し
③高リスクの低減策を取る



Guidelines of impact relevance for IHE profiles

Types of profile / Types of impact	Content profile	Workflow profile	Infrastructure profile
Loss of public trust, reputation	Relevant	Very relevant	Relevant
Loss of privacy	Less relevant	Very relevant	Very relevant
Loss of availability	Less relevant	Relevant	Very relevant
Loss of data integrity	Very relevant	Relevant	Very relevant
Loss of accountability or system integrity	Less relevant	Less relevant	Very relevant
Loss of confidentiality (i.e. Sensitive but not personal)	Less relevant	Very relevant	Very relevant
Loss of provider effectivness	Very Relevant	Very Relevant	Relevant
Loss / Decrease of program effectivness or viability	Relevant	Relevant	Relevant
Cost of incident response, fix, compliance orders	Relevant	Relevant	Very Relevant
Loss / Decrease of system effectivness or viability	Relevant	Relevant	Relevant
Legal liability / compensation	Very Relevant	Very Relevant	Relevant
Loss of life or quality of life	Very Relevant	Very Relevant	Very Relevant
Loss / Decrease in funding	Relevant	Relevant	Relevant
Accountable employees loose job	Relevant	Relevant	Relevant
Decrease in employee morale	Less relevant	Less relevant	Less relevant

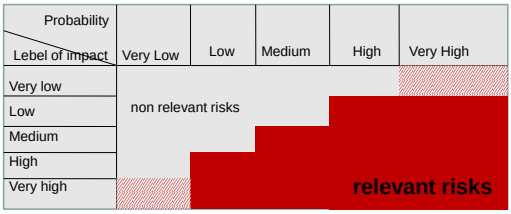
Example of level of impact

	Reputation	Delivery interruption scope
Very High	Potential for reduction in SSHA mandate	May not be able to deliver on most critical requirements
High	Serious adverse attention from media, medical establishment and / or public	Major shortfalls in one or more critical requirements
Medium	Minor adverse attention from media, medical establishment and / or public	Minor shortfalls in one or more key requirements
Low	Loss of reputation among clients / partners	A few shortfalls in desired functionality
Very Low	Internal loss of reputation	System should still fully meet mandatory requirements

Example of probability of occurrence

	Likelihood Description
Very High	This event will probably occur in the near future.
High	This event is likely to occur in the near future.
Medium	This event may occur in the near future.
Low	This event is possible but highly unlikely to occur in the near future.
Very Low	This event is not expected to occur in the near future.

Example of matrix for relevant risks identification



リスクの低減策

Mandate or suggest grouping of actors with IHE security profiles

• ATNA for:

• XUA for conveying of an authentication (against unauthorized access from a user point of view);

• DSG for:

• CT for sharing of consistent time (against attempt to thwart audit trails through desynchronization of actors' clocks);

• EUA for authentication within an enterprise (against masquerade).

Integrate security features in the profiles

Assign the mitigation of the risk to an identified agent (e.g. product developers, administrative procedures...)

Template for XDS Affinity Domain Deployment Planning

December 2.2008

Contents(1)

Contents(2)

Contents(3)

Contents(4)

Contents(5)

XADにおける機能的役割

Functional Role	説明
ケアの対象	EHRの主たるデータ対象
ケア提供機関の対象	患者、保護者、介護人、法的な代理人
個人的なヘルスケア専門家	患者のGP（かかりつけ医）が近い
権利をもつヘルスケア専門家	ケアの対象によって選ばれる
ヘルスケア専門家	患者を直接ケアする場合に部分的に含まれる
ヘルス関連専門家	患者ケア、教育、研究などで間接的に含まれる
行政	患者へのサービス提供を支援するその他の団体

Business Actor	Definition	Technical Actors	Actor Optionality	Comments
地域のHIE (State/Provincial, Regional, or Local)	共有サービスプロバイダ： 患者ID相互参照 マネージャ ポリシーリポジトリ 同意リポジトリ 監査リポジトリ レジストリ(可能性あり)	PIX manager PDQ Supplier ATNA Audit Repository XDS Registry XUA Service Provider	R/O/C R/O/C R/O/C R/O/C R/O/C	アクタが条件付きの場合は要求事項を書く テクニカルアクタの仕様のところに詳細を書く

Business Actor	Definition	Technical Actors	Actor Optionality	Comments
地域のドキュメントリポジトリ	リポジトリサービスをする地域の医療プロバイダ ドキュメントレジストリを含む 別々のレジストリに登録される場合もある	XDS-MS:ドキュメントの転送と共有 XDS-I ATNA 監査リポジトリとネットワークセキュリティ	R/O/C R/O/C R/O/C	

Business Actor	Definition	Technical Actors	Actor Optionality	Comments
記録を取得するヘルスケア提供者(ドキュメントコンシューマ)	HIEメンバーのリスト（情報取得することが認められている）を提供	XDS Document Consumer XDS-I Imaging Document Consumer XDS Document Source XDS-I Imaging Document Source ATNA Source Node PIX Consumer PDQ Consumer	R/O/C R/O/C R/O/C R/O/C R/O/C R/O/C R/O/C	

Business Actor	Definition	Technical Actors	Actor Optionality	Comments
医療記録を発行するヘルスケア提供者 (Document Source)	提供者のリスト(記録の発行が認められている)	XDS Document Source XDS-I Imaging Document Source ATNA Secure Node	R/O/C R/O/C R/O/C	
情報を提供する地域の行政機関 (Document Source)	州の行政機関のリスト(記録を発行することが認められている)	XDS Document Source XDS-I Imaging Document Source ATNA Secure Node	R/O/C R/O/C R/O/C	

F.2 IHE IT Infrastructure Technical Framework

「ITI User Handbook の 1 つで、複数医療機関での連携システム構築時にきめるべき “合意文書”の事項が解説と共に説明されている。

日本においても実際の構築時には参考資料として役立つ内容である。本書は項目とその概要を訳したものである。

IHE IT Infrastructure Technical Framework

Template for XDS Affinity Domain Deployment Planning

Version 15.0

December 2, 2008

1. はじめに(Introduction)

XAD のコンセプトは ITI TF-1:10 と Appendix K に定義されている。

多くの監視・専門組織にとって、コード化された用語、個人情報保護、文書形式と内容、言語サポート等についての方針が定義されていることが必要である。

本書は、ある地域における独立した XAD、多重の XAD の方針を定義する場合に使われるべき雛形である。実装決定、方針、XDS と関連 Profile の精密化を決めるための一貫した文書形式を示す。

Expected Knowledge and References としては、 XDS、PIX、PDQ、ATNA がある。

さらに、ISO/TS22600-1:2006 Privilege Management and Access Control, Part1:Overview and Policy management (cross border でのデータ交換におけるシナリオとクリティカルパラメータを記載)を参照。

2 目標(Goals)

・XAD の構築時に考慮すべき XDS と関連 Profile 領域の定義
・XAD の方針を定義する場合の標準的文書の雛形の提供

2.1 Request for Feedback

2.2 Open Issues and Questions

3 Overview

既存の ITI TF Appendix L にあるチェックリストでは不十分である。本書が Appendix L に置換る事が提案されている。

Appendix A: XDS Affinity Domain Definition Template

本 Template は、単独または複数の XAD において、実装の決定、ポリシー、IHE Profile の精密化の一貫した文書化の雛形を提供する。
さらに、XAD の構築で考慮すべき全関連トピックスのリストと、実装者にとってはポリシーと洗練された決定をガイドする際に役立つことを目指している。
本 Template の全項目が各 XAD において定義されている必要は無い。

A.1 はじめに(Introduction)
XDS Profile に拡張があるならば、ここに記載する。
XAD の拡張が国レベルで定義され、国に公式 IHE 組織があるならば、この組織が拡張を承認るものとし、ここに指定するものとする。拡張機能が承認される前に、テストの必要性を判断するのはこの組織の責任である。

A.2 用語(Glossary)
A.2.1 Terms
Access Control、Accountability
A.2.2 Abbreviations
EHR、HIE、IHE、PER、etc.

A.3 参考資料(Reference Documents)
XAD拡張での参照ドキュメント、拡張の意味を示すドキュメントのリスト。

A.4 組織的規約(Organizational Rules)
XAD 組織構造を定義する。
資金提供者、管理者と運営者の一覧、各役割と責任を明確に定義し、契約文書にすべきである。XAD への加入希望者が、加入情報を得たり XAD にアクセスしたりするために接触をすべき対象を明確にすべきである。
A.4.1 Organizational Structure
A.4.2 組織構成(Organizational Roles)
XAD の実装に関して経済的考慮事項を説明するものとする。
資金(公的/私的、税、など)、ビジネスモデル、運用と補修の会計計画を含む。
A.4.3 資金(Funding)
A.4.3.1 Fee Structure
A.4.3.2 Re-Imbursement Policies
A.4.3.3 Insurance Policies
A.4.3.4 Fiscal plan for System Operation, Maintenance, and Innovation
A.4.4 透明性(Transparency)
正確でタイムリな情報開示の方法が文書化されるものとする。
A.4.5 施行と是正(Enforcement and Remedies)
XADに関する施行規約(支払い、アクセス権限、パフォーマンスの要求、セキュリティ等)の責任組織の在り処を明確にする。
A.4.6 法的問題(Legal Issues)
A.4.6.1 法的統治性(Legal Governance)
ユーザ、出版者、IT スタッフ、ベンダに関係する法的事項の管理に関する方針の定義。
A.4.6.2 Government Regulations
A.4.6.3 義務とリスク配分(Liability and Risk Allocation)
A.4.6.4 免責(Indemnification)

XDS の実装に関する免責事項を記載する。本項に書くべき事項のガイドとして、以下の例がある。
・利用者によるデータ誤使用への法的告訴に対しての、提供者の免責
・患者からデータ誤利用に対しての告訴時、賠償責任を回避する仕組み
・データ提供者と全利用者間の免責の取決め
・データ使用以上に、公表についての問題を話す方法

A.4.6.5 発行物への知的財産権
(Intellectual Property Rights to Published Documents)

A.5 運用規則(Operational Rules)
A.5.1 サービスレベルの合意(Service Level Agreements)
A.5.2 日常的運営(Daily Governance)
XDS の運営レベルでの管理方法を記載する。
A.5.2.1 Policy Governance
A.5.2.2 Policy Change Procedures
A.5.2.3 Publication and Notification Policies
A.5.2.4 システム停止の管理(Management When Systems are Unavailable)
XAD の各構成要素が使用不可である場合の管理方針を定義する。例えば、PIX が利用できない場合、予定されたダウンタイムの通知方法、予定外のシステムダウンの原因と解決の通知、など。
A.5.3 構成管理(Configuration Management)
H/W や S/W の機能更新、構成変更等の管理方法を定義する。他要素への影響(停止をもたらすかもしれない、機能や構成の変更を必要とする)要素を変更するために必要な承認は何かを説明する。X.10 を参照する。
A.5.4 新機能要素の追加(Addition of New Components)
XAD への新要素の追加手続きを定義する。XAD の新要素追加の方法。新要素の認可をする組織は何処かを説明する。
Repository の追加、他 Repository への統合、XDS-I のローカルと集中アーカイバ間の移行。
A.5.5 データ維持、保存、バックアップ
(Data Retention, Archive, and Backup)
監査証跡の扱いと保持期間
A.5.6 不具合の回復(Disaster Recovery)

A.6 メンバの規約(Membership Rules)
A.6.1 入会(Acceptance)
XAD のメンバに加わり、構成要素とデータにアクセスできる組織、個人のタイプを定義する。
A.6.2 メンバのタイプ(Types of Membership)
公表データへのアクセス可能性（例、読取のみ、発表のみ、等）を定義するメンバ資格タイプの有無。
A.6.3 メンバ方針(Membership Policies)
メンバの状況を管理する規約を定義する。

A.7 XAD の外部からの接続性
(Connectivity To the XDS Affinity Domain from External Systems)
A.7.1 相互運用性規約(Interoperability Strategy)
ドメイン境界を越えたデータアクセス方法の手順が規定されるものとする。
A.7.1.1 External Connectivity Through Portals

A.8 システム構造(System Architecture)
情報の訂正と公表の安全性のために、AP のシステム構造が全参加者によって特定され理解されていなければならない。ポリシー合意文書は、種々の

Actor/Profile をサポートするシステムの構造、文書タイプと公表方針に関しての詳細を含むものとする。

A.8.1 全体構造(Global Architecture)

利害関係者、システム機能要素を含む全体のダイアグラムが記載されるべきである。XDS-I の Image データの置き場(ローカルか地域アーカイバか)。

A.8.2 XADのアクタ(Affinity Domain Actors)

XAD Integration Profile で定義される IHE アクタの実装に当たっては、システム通信上で特定できる必要がある。

A.8.2.1 Business Actors

A.8.2.2 Technical Actor Specifications

A.8.2.2.1 XDSドキュメントレジストリ(XDS Document Registry)

A.8.2.2.2 XDSドキュメントリポジトリ(XDS Document Repository)

A.8.2.2.3 XDSドキュメントソース(XDS Document Source)

A.8.2.2.4 XDS-Iドキュメントソース(XDS-I Imaging Document Source)

A.8.2.2.5 XDSドキュメント利用者(XDS Document Consumer)

A.8.2.2.6 XDS-Iドキュメント利用者(XDS-I Imaging Document Consumer)

A.8.2.2.7 XDS Patient Identity Source

A.8.2.2.8 PIX患者IDソース(PIX Patient Identity Source)

A.8.2.2.9 PIXマネージャ(PIX Manager)

A.8.2.2.10 PIX利用者(PIX Consumer)

A.8.2.2.11 PDQ Patient Demographics Supplier

A.8.2.2.12 PDQ Patient Demographics Consumer

A.8.2.2.13 ATNA Audit Record Repository

A.8.2.2.14 ATNA Secure Node

A.8.2.2.15 Secure Application

A.8.2.2.16 CT Time Server

A.8.2.2.17 CT Time Client

A.8.2.2.18 Any Additional IHE Actor Systems

A.8.2.2.19 Additional Affinity Domain Specific Recognized Technical Actors

A.8.2.3 XADトランザクション(XDS Affinity Domain Transaction Diagram)

XAD の通信ダイアグラムを定義する。特に、XAD 拡張では必須として定義している付加的通信の詳細は重要である。

A.8.2.4 XAD間のトランザクション
(Cross XDS Affinity Domain Transaction Support)

この XAD には属さない外部システムへの通信に必要な詳細を規定する。
“異なる code sets”、さらに” ID 認証の妥当性”を扱う手続きを説明する。

A.9 用語と意味(Terminology and Content)

A.9.1 はじめに(Introduction)

XAD で精密化される用語と内容の基本部分を説明する。

A.9.1.1 識別構成の共通規約
(Common Rules for Identifier Construction (example))

例えば、OID の生成規約を指定する。

OID:ISO オブジェクト識別子で、64 字以内の数字とピリオッド。

A.9.2 Data Content Rules and Restrictions

A.9.2.1 Example of Rules and Restrictions for Patient Demographic Data

A.9.3 レジストリのメタデータ(XDS Registry Metadata)

A.9.3.1 XDS Document Entry Metadata

ITI TF-2: Table 4.15 にある Document Metadata Attribute Definitions の定義をする。

A.9.3.1.1 作成組織名の精密化
(Refinement of author Institution (example))

XON:HL7 V2 Organization Name の第一コンポーネントで指定する組織名。
A.9.3.1.1.1 組織名要素の精密化
(Refinement of Organization Name component (example))
A.9.3.1.1.2 その他(Etc.)
A.9.3.1.2 ドキュメントエントリ属性の精密化
(Refinement of Further XDS Document Entry Attributes (example))
A.9.3.2 XDS Submission Set Metadata
ITI TF-2: Table 4.1-6 Submission Set Metadata Attribute Definitions の定義をする。
A.9.3.2.1 Refinement of Submission Set Metadata Attributes (example)
A.9.3.3 フォルダのメタデータ(Folder Metadata)
ITI TF-2: Table 3.14.4.1-7 Folder Metadata Attribute Definitions の定義をする。
A.9.3.3.1 codeListの精密化(Refinement of codeList (example)
A.9.4 サポートする内容(Supported Content)
A.9.4.1 サポートするプロファイル(Supported Content Profiles)
XDS-MS,XDS-SD,XDS-I,XDS-BPPC,XDS-*,等
A.9.4.1.1 XDS-MS Document Content Refinement (Example)

A.10 プライバシ(Patient Privacy and Consent)
A.10.1 ドキュメントのアクセスと利用の一般則
(General Guidelines Regarding Document Access and Use)
XAD の情報へのアクセスと利用に関する一般側を定義する。BPPC の Privacy Access Policy では、いくつかの例を示している。
アクセス権限が利用者の役割に結びついているならば、アクセスが許されるドキュメント種別に対する利用者の役割を規定するアクセス制御マトリックスが決められるべきである。
A.10.2 患者同意(Patient consent)
A.10.2.1 BPPC
BPPC Profile のサポートをしなければならないか否かを決める。BPPC 利用のルールを定義する。
A.10.3 プライバシを越える時のガイド(Privacy Over-ride Guidelines)
緊急時、グレークグラス、システム停止、等の条件を特定する。

A.11 技術的セキュリティ(Technical Security)
各ドメインでは独自のセキュリティルールを用いがちであるが、同一のセキュリティモデルを使うことが望ましい。CEN、ISO で定義された security standard が最初のゴールである。
A.11.1 認証(Authorization)
A.11.1.1 役割管理(Role Management)
A.11.1.1.1 Functional Roles
A.11.1.1.2 Structural Roles
A.11.1.2 役割識別(Authentication of Users/Role)
パスワード規約、2要素、認証、等の識別方法。
A.11.1.2.1 ユーザ・役割の認証管理(User/Role Certificates management)
A.11.1.3 証明書権限(Attestation rights)
A.11.1.4 委任権限(Delegation rights)
A.11.1.5 時間有効性(Validity time)
認証等の有効な時間を決めなければならない。
A.11.2 ノード識別(Node Authentication)
A.11.2.1 ノード認証(Node Certificates Management)
A.11.3 情報アクセス(Information Access)
A.11.3.1 監査証跡アクセス(Security Audit Log Access)
A.11.3.2 ネットワークのセキュリティ要件

(Network Communication Access Security Requirements)
XADでのネットワークアクセスのセキュリティ要件を特定する。
A.11.3.3 ノードアクセスのセキュリティ要件
(Node Access Security Requirements)
例えば、全ノードがATNA Profileに従う必要が有るか否か。
A.11.3.4 可搬媒体のセキュリティ要件
(Removable Media Access Security Requirements)
A.11.3.5 取決めの更新周期(Agreement validity period)
取決め内容の有効期限は、その取決め内で規定するものとする。
A.11.4 情報の完全性(Information Integrity)
X.10.4.1 ネットワークの完全性要件
(Network Communication Integrity Requirements)
完全性チェックに使われる方法。
A.11.4.2 ディジタル署名
(Document Digital Signature Requirements/Policy)
A.11.4.3 更新と保守方針 (Document Update and Maintenance Policies)
A.11.4.3.1 訂正方針(Document Correction Policy)
A.11.4.3.2 更新方針(Document Update Policy)
A.11.4.3.3 アクセス方針(Document Read Policy)
A.11.4.3.4 削除方針(Document Deletion Policy)
A.11.4.4 フォルダの方針(Folder Update and Maintenance Policies)
A.11.4.4.1 Folder Correction Policy
A.11.4.4.2 Folder Update Policy
A.11.4.4.3 Folder Read Policy
A.11.4.4.4 Folder Deletion Policy
A.11.5 倫理(Ethics)
規則と規制だけでは全ての状況をカバーできない。それ故に、倫理が考慮され、全員が共同する責任の枠組に関して全員によく理解してもらうための覚書が公式化されるべきである。
A.11.6 監査証跡(Secure Audit Trail)
全 transaction は ATNA Profile を使ってログされるものとする。旧来のシステムが ATNA を備えていなければ、サポートの仕方を定義するものとする。
A.11.7 (Consistent Time)
CT Profile のサポート方法を規定する。
A.11.8 監査(Audit check)
何時、誰が監査し、適切な行動が取られるかが合意されるものとする。
A.11.9 リスク分析(Risk analysis)
少なくとも、年1度は見直すものとする。
A.11.9.1 General Mitigations
A.11.9.1.1 Common Criteria (ISO/IEC 15408)
A.11.9.2 Identified Risks
A.11.10 将来のシステム拡張(Future system developments)

附属書 G.　提案依頼事項について

本附属書では、システム発注時に考慮するべき、提案依頼事項について述べる。地域医療連携情報システムに限らず、製品導入の際には開発企業が信頼できるかを確認することが重要である。

主に下記については、仕様書に提出を明記して、技術審査に用いる。

- 品質管理体制
  - 開発業者の製品に対する品質管理体制の説明資料
- 開発体制および開発実績
  - 製品開発に関わる者の過去の開発実績に関する説明資料
- 技術者スキル
  - 情報工学、医療情報などに関する保有資格
  - プログラム開発に従事した年数
  - 使用できるコンピュータ言語
- 個人情報保護方針および情報セキュリティ管理体制
  - 開発業者の情報セキュリティ管理体制に関する説明資料
  - 開発業者の個人情報保護方針に関する説明資料
- 保守体制
  - 電話対応可能時間
  - 夜間・休日の対応
  - 定期点検方法

製品を長期的に維持・管理するために、開発企業に開発体制や技術者のスキル、品質維持の仕組み、保守体制などを説明する資料を提出させる必要がある。

技術者のスキルには、情報処理技術や医療情報、医療に関して取得している資格や製品開発に携わっている年数を説明させる。

本ハンドブックは、厚生労働省事業により支援を受けて作成しました。

2010 年 4 月 20 日発行

地域医療連携情報システム構築
ハンドブック 2010
―IHE XDS による HIE（Health Information Exchange）の構築―